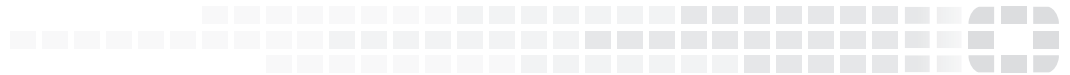




**FORTINET**



# FortiOS™ Handbook - Virtual FortiOS

VERSION 6.0.2

**FORTIOS  
VERSION  
6.0**

## **FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

## **FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

## **FORTINET KNOWLEDGE BASE**

<http://kb.fortinet.com>

## **FORTINET BLOG**

<https://blog.fortinet.com>

## **CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

## **FORTINET COOKBOOK**

<http://cookbook.fortinet.com>

## **FORTINET TRAINING AND CERTIFICATION PROGRAM**

<https://www.fortinet.com/support-and-training/training.html>

## **NSE INSTITUTE**

<https://training.fortinet.com/>

## **FORTIGUARD CENTER**

<https://fortiguard.com>

## **FORTICAST**

<http://forticast.fortinet.com>

## **END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>



July 26, 2018

FortiOS™ Handbook - Virtual FortiOS

01-602-481103-20180726

# TABLE OF CONTENTS

<b>Change log</b>	<b>5</b>
<b>Introduction</b>	<b>6</b>
Document scope	6
What's new in virtual FortiOS 6.0.2	6
What's new in virtual FortiOS 6.0.1	6
What's new in virtual FortiOS 6.0	7
<b>Virtual FortiOS overview</b>	<b>8</b>
FortiGate VM models and licensing	8
FortiGate VM evaluation license	9
VM licenses and vCPUs	9
Registering FortiGate VM	10
Downloading the FortiGate VM deployment package	10
Deployment package contents	12
Citrix XenServer	12
OpenXEN	12
Microsoft Hyper-V	12
KVM	12
VMware ESX/ESXi	12
Deploying the FortiGate VM appliance	13
Performance and optimization	14
Interrupt affinity	14
Packet distribution	14
Other virtual FortiOS products	15
SDN environments	15
Public cloud environments	18
<b>Deployment example – VMware</b>	<b>25</b>
Open the FortiGate VM OVF file with the vSphere client	25
Configure FortiGate VM hardware settings	31
Transparent mode VMware configuration	32
High availability VMware configuration	33
Power on your FortiGate VM	33
<b>Deployment example – MS Hyper-V</b>	<b>34</b>
Create the FortiGate VM virtual machine	34
Configure FortiGate VM hardware settings	41

FortiGate VM virtual processors .....	43
FortiGate VM network adapters .....	44
FortiGate VM virtual hard disk .....	45
High availability Hyper-V configuration .....	52
Start the FortiGate VM .....	53
<b>Deployment example – KVM .....</b>	<b>54</b>
Create the FortiGate VM virtual machine .....	54
Configure FortiGate VM hardware settings .....	56
Start the FortiGate VM .....	57
<b>Deployment example – Open Xen .....</b>	<b>58</b>
Create the FortiGate VM virtual machine .....	58
<b>Deployment example – Citrix XenServer .....</b>	<b>64</b>
Create the FortiGate VM virtual machine (XenCenter) .....	64
Configure virtual hardware .....	68
Configuring number of CPUs and memory size .....	68
Configuring disk storage .....	69
<b>FortiGate VM initial configuration .....</b>	<b>71</b>
Set FortiGate VM port1 IP address .....	71
Connect to the FortiGate VM web-based manager .....	74
Upload the FortiGate VM license file .....	74
GUI .....	74
CLI .....	75
Validate the FortiGate VM license with FortiManager .....	76
To validate your FortiGate VM with your FortiManager: .....	76
Licensing timeout .....	77
Configure your FortiGate VM .....	77

## Change log



Date	Change description
July 26, 2018	FortiOS 6.0.2 document release. See <a href="#">What's new in virtual FortiOS 6.0.2 on page 6</a> .
June 5, 2018	FortiOS 6.0.1 document release. See <a href="#">What's new in virtual FortiOS 6.0.1 on page 6</a> .
March 29, 2018	FortiOS 6.0 document release. See <a href="#">What's new in virtual FortiOS 6.0 on page 7</a> .

# Introduction

FortiGate virtual appliances allow you to mitigate blind spots by implementing critical security controls within your virtual infrastructure. They also allow you to rapidly provision security infrastructure whenever and wherever it is needed. FortiGate virtual appliances feature all of the security and networking services common to traditional hardware-based FortiGate appliances. With the addition of virtual appliances from Fortinet, you can deploy a mix of hardware and virtual appliances, operating together and managed from a common centralized management platform.

## Document scope

This document describes how to deploy a FortiGate virtual appliance in several virtualization server environments. This includes how to configure the virtual hardware settings of the virtual appliance.

This document assumes:

- you have already successfully installed the virtualization server on the physical machine,
- you have installed appropriate VM management software on either the physical server or a computer to be used for VM management.

This document does not cover configuration and operation of the virtual appliance after it has been successfully installed and started. For these issues, see the FortiGate Handbook.

This document includes the following sections:

- [Virtual FortiOS overview](#)
- [Deployment example – VMware](#)
- [Deployment example – MS Hyper-V](#)
- [Deployment example – KVM](#)
- [Deployment example – Open Xen](#)
- [Deployment example – Citrix XenServer](#)

## What's new in virtual FortiOS 6.0.2

The following list contains new firewall features added in FortiOS 6.0.2. Click on a link to navigate to that section for further information.

- Allow public cloud customers to use the licensed number of vCPUs on a virtual instance even if there are more vCPUs than licensed for. For more information see [VM licenses and vCPUs on page 9](#)

## What's new in virtual FortiOS 6.0.1

The following list contains new firewall features added in FortiOS 6.0.1. Click on a link to navigate to that section for further information.

- [SDN connector support on page 23](#)
- [Tagging NSX VMs from FortiGate on page 16](#)
- [AWS GuardDuty integration on page 19](#)
- [HA support for Oracle Cloud Infrastructure on page 24](#)

## What's new in virtual FortiOS 6.0

The following list contains new firewall features added in FortiOS 6.0. Click on a link to navigate to that section for further information.

- [FortiOS On-Demand supported platforms on page 15](#)
- [NSX credentials encryption on page 17](#)
- [Certificate validation to NSX manager on page 17](#)
- [FortiGate VMX license status](#)
- [SDN connector addressing on page 17](#)
- [Support for KVM-based hypervisor in AWS on page 18](#)
- [HA support for GCP on page 22](#)
- [HA support for Azure on page 20](#)

# Virtual FortiOS overview

The following topics are included in this section:

- [FortiGate VM models and licensing](#)
- [Registering FortiGate VM](#)
- [Downloading the FortiGate VM deployment package](#)
- [Deployment package contents](#)
- [Deploying the FortiGate VM appliance](#)
- [Performance and optimization](#)
- [Other virtual FortiOS products](#)

## FortiGate VM models and licensing

Fortinet offers the FortiGate VM in five virtual appliance models determined by license. When configuring your FortiGate VM, be sure to configure hardware settings within the ranges outlined below. Contact your Fortinet Authorized Reseller for more information.

### FortiGate VM model information

Technical Specification	FG-VM00	FG-VM01	FG-VM02	FG-VM04	FG-VM08	FG-VM16	FG-VM32	FG-VMUL
Virtual CPUs (min / max)	1 / 1	1 / 1	1 / 2	1 / 4	1 / 8	1 / 16	1 / 32	1 / unlimited
Virtual Network Interfaces (min / max)	2 / 10							
Virtual Memory (min / max)	1GB / 2GB	1GB / 2GB	1GB / 4GB	1GB / 6GB	1GB / 12GB	1GB / 24GB	1GB / 48GB	1GB / unlimited GB
Virtual Storage (min / max)	32GB / 2TB							
Managed Wireless APs (tunnel mode / global)	32 / 32	32 / 64	256 / 512	256 / 512	1024 / 4096	1024 / 4096	1024 / 4096	1024 / 4096
Virtual Domains (default / max)	1 / 2	10 / 10	10 / 25	10 / 50	10 / 500	10 / 500	10 / 500	10 / 500





There may be times the min/max values can change. An example for this is when the maximum memory for FG-VM00 changed between 5.2 and 5.4 from 1 GB to 1.5 GB. If that is the case, the settings for the VM will have to be manually changed to accommodate the new parameters.

After placing an order for FortiGate VM, a license registration code is sent to the email address used on the order form. Use the registration number provided to register the FortiGate VM with Customer Service & Support and then download the license file. Once the license file is uploaded to the FortiGate VM and validated, your FortiGate VM appliance is fully functional.

## FortiGate VM evaluation license

FortiGate VM includes a limited embedded 15-day trial license that supports:

- 1 CPU maximum
- 1024 MB memory maximum
- low encryption only (no HTTPS administrative access)
- all features except FortiGuard updates

You cannot upgrade the firmware, doing so will lock the Web-based Manager until a license is uploaded. Technical support is not included. The trial period begins the first time you start FortiGate VM. After the trial license expires, functionality is disabled until you upload a license file.



The number of Virtual Network Interfaces is not solely dependent on the FortiGate VM. Some virtual environments have their own limitations on the number of interfaces allowed. As an example, if you go to <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-multiple-nics>, you will find that Azure has its own restrictions for VMs, depending on the type of deployment or even the size of the VM.

## VM licenses and vCPUs

The primary requirement for the provisioning of a virtual FortiGate may be the number of interfaces it can accommodate rather than its processing capabilities. In some cloud environments, the options with a high number of interfaces tend to have high numbers of vCPUs.

### FortiOS 6.0.1 and earlier

Previously, if you needed a virtual instance with a high number of interfaces you needed to purchase a FortiGate-VM license for a high number of vCPUs regardless of whether you needed the processing power. If you attempt to install FortiGate-VM, licensed for a specific number of vCPUs on a public cloud instance that is configured with more vCPUs than the FortiGate is licensed for, the instance will not run.

#### Example for FortiOS 6.0.1 and earlier

License	1 vCPU	2 vCPU	4 vCPU	8 vCPU	16 vCPU	32 vCPU
FGT-VM08	OK	OK	OK	OK	Will not run	Will not run

## FortiOS 6.0.2 and later

The licensing for FortiGate-VM does not restrict whether the FortiGate can work on a VM instance in a public cloud that uses more vCPUs than the license allows. The number of vCPUs indicated by the license does not restrict the FortiGate from working, regardless of how many vCPUs are included in the virtual instance. However, only the licensed number of vCPUs process traffic. The rest of the vCPUs are used for management.

### Example for FortiOS 6.0.2 and later

License	1 vCPU	2 vCPU	4 vCPU	8 vCPU	16 vCPU	32 vCPU
FGT-VM08	OK	OK	OK	OK	8 vCPUs used for traffic. The rest are allocated for management	8 vCPUs used for traffic. The rest are allocated for management.

You can provision a VM instance based on the number of interfaces you need and license the FortiGate-VM for only the processors you need.

## Registering FortiGate VM

To obtain the FortiGate VM license file you must first register your FortiGate VM with the [Fortinet Support](#) website.

### To register your FortiGate VM:

1. Log in to the Customer Service & Support portal using an existing support account or select **Sign Up** to create a new account.
2. In the main page, under **Asset**, select **Register/Renew**.

The **Registration** page opens.

3. Enter the registration code that was emailed to you and select **Register**. A registration form will display.
4. After completing the form, a registration acknowledgment page will appear.
5. Select the **License File Download** link.
6. You will be prompted to save the license file (.lic) to your local computer. See "Upload the license file" for instructions on uploading the license file to your FortiGate VM via the Web-based Manager.

## Downloading the FortiGate VM deployment package

FortiGate VM deployment packages are included with FortiGate firmware images on the [Customer Service & Support](#) site. First, see the following table to determine the appropriate VM deployment package for your VM platform.

## Selecting the correct FortiGate VM deployment package for your VM platform

VM Platform	FortiGate VM Deployment File
Citrix XenServer v5.6sp2, 6.0 and later	FGT_VM64-v500-buildnnnn-FORTINET.out.CitrixXen.zip
Open Xen v3.4.3, 4.1	FGT_VM64-v500-buildnnnn-FORTINET.out.OpenXen.zip
Microsoft Hyper-V Server 2008R2 and 2012	FGT_VM64-v500-buildnnnn-FORTINET.out.hyperv.zip
KVM (qemu 0.12.1)	FGT_VM64-v500-buildnnnn-FORTINET.out.kvm.zip
VMware ESX 4.0, 4.1 ESXi 4.0/4.1/5.0/5.1/5.5	FGT_VM32-v500-buildnnnn-FORTINET.out.ovf.zip (32-bit)
	FGT_VM64-v500-buildnnnn-FORTINET.out.ovf.zip

For more information see the FortiGate product datasheet available on the Fortinet web site, [https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate\\_VM.pdf](https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_VM.pdf).

The firmware images FTP directory is organized by firmware version, major release, and patch release. The firmware images in the directories follow a specific naming convention and each firmware image is specific to the device model. For example, the FGT\_VM32-v500-build0151-FORTINET.out.ovf.zip image found in the v5.0 Patch Release 2 directory is specific to the FortiGate VM 32-bit environment.



You can also download the FortiOS Release Notes, FORTINET-FORTIGATE MIB file, FSSO images, and SSL VPN client in this directory. The Fortinet Core MIB file is located in the main FortiGate v5.00 directory.

### To download the FortiGate VM deployment package:

1. In the main page of the Customer Service & Support site, select **Download > Firmware Images**.

The **Firmware Images** page opens.

2. In the **Firmware Images** page, select **FortiGate**.
3. Browse to the appropriate directory on the FTP site for the version that you would like to download.
4. Download the appropriate .zip file for your VM server platform.

You can also download the FortiGate Release Notes.

5. Extract the contents of the deployment package to a new file folder.

## Deployment package contents

### Citrix XenServer

The FORTINET.out.CitrixXen.zip file contains:

- fortios.vhd: the FortiGate VM system hard disk in VHD format
- fortios.xva: binary file containing virtual hardware configuration settings
- in the ovf folder:
  - FortiGate-VM64.ovf: Open Virtualization Format (OVF) template file, containing virtual hardware settings for Xen
  - fortios.vmdk: the FortiGate VM system hard disk in VMDK format
  - datadrive.vmdk: the FortiGate VM log disk in VMDK format

The ovf folder and its contents is an alternative method of installation to the .xva and VHD disk image.

### OpenXEN

The FORTINET.out.OpenXen.zip file contains only fortios.qcow2, the FortiGate VM system hard disk in qcow2 format. You will need to manually:

- create a 32GB log disk
- specify the virtual hardware settings

### Microsoft Hyper-V

The FORTINET.out.hyperv.zip file contains:

- in the Virtual Hard Disks folder:
  - fortios.vhd: the FortiGate VM system hard disk in VHD format
  - DATADRIVE.vhd: the FortiGate VM log disk in VHD format
- In the Virtual Machines folder:
  - fortios.xml: XML file containing virtual hardware configuration settings for Hyper-V. This is compatible with Windows Server 2012.
- Snapshots folder: optionally, Hyper-V stores snapshots of the FortiGate VM state here

### KVM

The FORTINET.out.kvm.zip contains only fortios.qcow2, the FortiGate VM system hard disk in qcow2 format. You will need to manually:

- create a 32GB log disk
- specify the virtual hardware settings

### VMware ESX/ESXi

You will need to create a 32GB log disk.

The FORTINET.out.ovf.zip file contains:

- fortios.vmdk: the FortiGate VM system hard disk in VMDK format
- datadrive.vmdk: the FortiGate VM log disk in VMDK format
- Open Virtualization Format (OVF) template files:
  - FortiGate-VM64.ovf: OVF template based on Intel e1000 NIC driver
  - FortiGate-VM64.hw04.ovf: OVF template file for older (v3.5) VMware ESX server
  - FortiGate-VMxx.hw07\_vmxnet2.ovf: OVF template file for VMware vmxnet2 driver
  - FortiGate-VMxx.hw07\_vmxnet3.ovf: OVF template file for VMware vmxnet3 driver



Use the VMXNET3 interface (FortiGate-VMxx.hw07\_vmxnet3.ovf template) if the virtual appliance will distribute workload to multiple processor cores.

---

## Deploying the FortiGate VM appliance

Prior to deploying the FortiGate VM appliance, the VM platform must be installed and configured so that it is ready to create virtual machines. The installation instructions for FortiGate VM assume that

- You are familiar with the management software and terminology of your VM platform.
- An Internet connection is available for FortiGate VM to contact FortiGuard to validate its license or, for closed environments, a FortiManager can be contacted to validate the FortiGate VM license. See "Validate the FortiGate VM license with FortiManager".

For assistance in deploying FortiGate VM, refer to the deployment chapter in this guide that corresponds to your VMware environment. You might also need to refer to the documentation provided with your VM server. The deployment chapters are presented as examples because for any particular VM server there are multiple ways to create a virtual machine. There are command line tools, APIs, and even alternative graphical user interface tools.

Before you start your FortiGate VM appliance for the first time, you might need to adjust virtual disk sizes and networking settings. The first time you start FortiGate VM, you will have access only through the console window of your VM server environment. After you configure one FortiGate network interface with an IP address and administrative access, you can access the FortiGate VM web-based manager.

After deployment and license validation, you can upgrade your FortiGate VM appliance's firmware by downloading either FGT\_VM32-v500-buildnnnn-FORTINET.out (32-bit) or FGT\_VM64-v500-buildnnnn-FORTINET.out (64-bit) firmware. Firmware upgrading on a VM is very similar to upgrading firmware on a hardware FortiGate unit.



FortiGate-VM is not part of the FortiGuard Network for the purpose of upgrades.

---

## Performance and optimization

Performance is improved for FortiOS VM platforms by implementing features to improve efficiency and resource utilization.

### Interrupt affinity

You can configure interrupt affinity and packet distribution to optimize performance for your VM environment. Interrupt affinity allows you to align interrupts from interfaces to specific CPUs.

#### Configuring interrupt affinity

Use the following commands to configure interrupt affinity for two 10G interfaces (port2 and port3).

Interrupts from first interface are assigned to core #0 and those from the second interface are assigned to core #1.

```
config system affinity-interrupt
  edit 1
    set interrupt "port2-TxRx-0"
    set affinity-cpumask "0x1"
  next
  edit 2
    set interrupt "port2-TxRx-1"
    set affinity-cpumask "0x1"
  next
  edit 3
    set interrupt "port3-TxRx-0"
    set affinity-cpumask "0x2"
  next
  edit 4
    set interrupt "port3-TxRx-1"
    set affinity-cpumask "0x2"
end
```

### Packet distribution

Packet distribution allows you to configure FortiGate-VM to distribute processing to multiple CPUs. Use the following commands to configure packet redistribution to redistribute packets from core #0 and #1 to all other cores.

#### Configuring packet distribution

The example is based on VM08:

```
config system affinity-packet-redistribution
  edit 1
    set interface "port2"
    set affinity-cpumask "0xFC"
  next
  edit 2
    set interface "port3"
    set affinity-cpumask "0xFC"
end
```

## Other virtual FortiOS products

Just like a VM installed on a platform located on a physical computer, these are instances of the FortiOS firmware installed in virtual environments.

### SDN environments

FortiOS-VM is now supported in a Number of SDN (Software Defined Network) environments through the use of a SDN connector. The software can be found on the [Fortinet Service and Support site](#). Documentation can be found on the [Fortinet Documentation site](#) under the product heading of Fortinet Connectors.

The products include:

#### FortiGate-VMX

Admin guide can be found at <https://docs.fortinet.com/d/fortigate-vmx-install-v.2>.

#### FortiOS On-Demand

Admin guide can be found at <https://docs.fortinet.com/d/fortigate-fortinetvm-on-demand-administration-guide>.

#### FortiOS On-Demand supported platforms

##### Connectors:

##### FortiADC Connector for Cisco ACI

- Guides found at <https://docs.fortinet.com/fortinet-connectors/admin-guides>.
- Versions available:
  - 1.0.0
  - 1.2.0
  - 1.3.0

##### FortiADC Connector for Cisco ACI

- Guides found at <https://docs.fortinet.com/fortinet-connectors/admin-guides>.
- Versions available:
  - 1.0.0
  - 1.2.0
  - 1.3.0

##### FortiGate Connector for HPE VAN SDN

- Guides found at <https://docs.fortinet.com/fortinet-connectors/admin-guides>.
- Versions available:
  - 1.0.5
  - 1.1.0

##### FortiGate Connector for OpenStack ML2

- Guides found at <https://docs.fortinet.com/fortinet-connectors/admin-guides>.
- Versions available:

- 1.1

### FortiManager Connector for Nuage Networks

- Guides found at <https://docs.fortinet.com/fortinet-connectors/admin-guides>.
- Versions available:
  - 1.0

### Fortinet SDN Connector for Nuage VSP

Instruction can be found at <http://cookbook.fortinet.com/nuage-vsp/>

## Additional information relating to connectors

While the product documentation concerns itself with the connector software, there is also settings within FortiOS that relates to the usage of those connectors.

### NSX connector support

There is support for NSX connector to upgrade to SDN connectors.

#### Change to config system sdn-connector:

```
config nsx setting
```

#### Change to config firewall address:

```
set type nsx  
  
set type dynamic  
set sdn nsx
```



When using the sdn nsx setting, the user should also use the nsx rest-api password.

---

## Tagging NSX VMs from FortiGate

There is a requirement to have VMs tagged for the use of features such as IP detection. The tagging of VMs in an NSX environment is performed from the FortiGate by using an `execute` command.

The command performs the following functions when run:

- An API call to NSX to find the `vm_id` based on the IP address.
- An API call to resolve the security tag name to `tag_id`
- An API call to add the VM to the security tag

#### Command syntax:

```
execute sdn tag nsx <ip> <tagname> <enable or disable spoofguard>
```



Option	Description
<b>ip</b>	IP address of the VM
<b>tagname</b>	Name of tag for the VM(s)
<b>enable or disable spoofguard</b>	<ul style="list-style-type: none"> <li>• 1 is used to enable SpoofGuard</li> <li>• 0 is used to disable SpoofGuard</li> </ul>

### NSX credentials encryption

NSX requires AES256 as a minimum level of encryption. The credentials for NSX are stored using AES256 encryption in preparation for being transmitted over the network for NSX authentication.

### Certificate validation to NSX manager

The first time FortiGate-SVM connects to the NSX Manager (when a **Service Manager** is added), you can save the service manager's certificate as a fingerprint in the FortiGate configuration. After this is done, the FortiGate-SVM can validate the connection by matching the certificate of the NSX Manager against the saved fingerprint in the configuration every time that:

- the FortiGate-SVM connects to the NSX Manager
- the NSX Manager connects to the FortiGate-SVM

### CLI settings:

This setting is available only in the CLI.

```
config system sdn-connector
  edit <connector-name>
    set type nsx
    set nsx-cert-fingerprint <string value>
  end
```



`nsx-cert-fingerprint` is a hidden entry. If you are in the `nsx` context and type the command `set ?` to get a listing of the available options, it will not show up.

### Removal of fingerprint

If the NSX Manager service is deleted from the FortiGate-SVM, to avoid potential security issues, the fingerprint is automatically deleted.

### SDN connector addressing

When setting the address for an SDN connection, the value can be a fully qualified domain name (FQDN) as well as an IP address. The setting that is currently called `server` was once called `server-ip`.

### CLI

```
config system sdn-connector
  edit <example>
```

```
set server [<ip address>|<fqdn address>]
end
```

## Public cloud environments

Unlike SDNs where the user has administrative control over the virtual environment that the FortiOS is being placed into, the Public Cloud services are run and managed by 3rd party companies with their own methods and rules of provisioning that need to be followed to install the firmware into the environment.

### Amazon Web Services (AWS)

Online documentation can be found at <http://cookbook.fortinet.com/amazon-web-services-aws/>

#### Additional information for AWS

While the online documentation is primarily for the installation of the FortiOS into the virtual environment, periodically improvements are made to the firmware that affects its interaction with the environment but isn't really covered by installation instructions or information has changed in regards to those instructions but they may not have all been updated yet.

#### Support for KVM-based hypervisor in AWS

FortiGate-VM can be provisioned in AWS C5 instances on the marketplace (BYOL/OnDemand). These instances are based on a home-brewed version of KVM that AWS started using. Systems deployed in C5 will see better performance compared to C3/C4 instances. Deploying FortiGate-VM in these instances requires no configuration on the part of the user.

FortiGate-VM firmware can be placed in these instances because of:

- An NVME driver that is required to run C5 instances. It gets the correct partition name dependencies if an NVME device is being used.
- Removing the `xenstore` checking requirement in the AWS setup daemon that is not required in non-Xen based instances.

## HA

AWS supports the use of HA.

This includes two parts:

1. HA with unicast heartbeat traffic.
2. AWS API supports to move secondary IPs and update routing tables.

#### CLI:

Unicast HA config

```
config system ha
  unicast-hb {enable|disable}
  unicast-hb-peerip <Unicast Heartbeat Peer IP>
end
```

#### SDN connector - AWS

Improvements have been made in the support of FortiGate-VM integrating into the AWS environment.

1. `config aws setting` has been moved to the context of `config system sdn-connector`.
 

```
config system sdn-connector
  edit <string>
    set access-key <AWS access key ID>
    set secret-key <AWS secret access key>
    set region <AWS region name>
    set vpc-id <AWS VPC ID>
  end
```
2. Update to the GUI SDN connector edit page that supports allowing configuration of the following fields:
  - AWS access key ID
  - AWS secret access key
  - AWS region name
  - AWS VPC ID
  - Update Interval
3. Change to address edit page to allow configuration of the **Filter** field for Dynamic AWS address.
4. Update to the dynamic address monitor API to get resolved address list for dynamic AWS addresses.

### AWS GuardDuty integration

AWS GuardDuty is a managed threat detection service that monitors malicious or unauthorized behaviors/activities related to AWS resources. GuardDuty provides visibility of logs called findings, and Fortinet provides a Lambda script that populates a list of malicious IP addresses then stores it in an S3 location. FortiGate can then be configured to point to the location as the external feed of threat vectors.

To use this feature, you must subscribe to GuardDuty, CloudWatch, and S3.



Fortinet-provided Lambda scripts are not supported within regular Fortinet technical support scope. For questions related to the scripts, contact [awssales@fortinet.com](mailto:awssales@fortinet.com).

GuardDuty findings give visibility on the following:

- **Severity:** High/medium/low (associated with scores)
- **Where it occurred:** Region, resource ID, account ID
- **When:** Last seen date/time
- Count
- **Detailed information can include:**
  - **Affected resource:** type/instance ID/image ID/port/resource type/image description/launch time/tags/network interfaces (public IP, private IP, subnet ID, VPCID, security groups)
  - **Action:** type/connection direction
  - Actor
  - Additional information

#### To configure the integration:

- Subscribe and enable GuardDuty on AWS. When findings occur, they are pushed to CloudWatch.
- CloudWatch events trigger the Lambda script for automated actions.

- If one of the following criteria is met:
  - Connected direction is inbound, the finding contains an IPAddress, and the severity is greater than the minimum score (configurable)
  - Connected direction is unknown, the finding contains an IP address and matches certain known threat lists (such as ProofPoint) that GuardDuty identifies, and the severity is greater than the minimum score

The IP address is considered black and is appended to a file located in the S3 bucket/directory.

- FortiGate queries the file as the external source of blacklisted IP addresses. The following is an example configuration:

The screenshot shows the FortiGate GUI with the 'System' menu open and 'External Resources' selected. The 'Edit External Resource' window is displayed, showing the configuration for a resource named 'GuardDuty'. The 'Type' is set to 'Firewall IP Address'. The 'Name' is 'GuardDuty'. A note states: 'Resource name will appear as an "External IP Block List" in DNS Filter Profiles and as a "Source/Destination" in Proxy Policy.' The 'URI of external resource' is 'https://s3.us-east-2.amazonaws.com/ip'. The 'Refresh Rate' is '5'. The 'Comments' field is empty. The 'Last Update' status is 'Not updated'. The 'Status' is 'On'. The 'OK' and 'Cancel' buttons are at the bottom right.

The configuration can be done in the CLI as follows:

```
config system external-resource
  edit "GuardDuty"
    set type address
    set resource "https://s3.us-east-2.amazonaws.com/ip-blacklist/ip.txt"
  next
end
```

You can then use the gathered IP addresses as criteria to protect the network.

## Azure

### HA support for Azure

FortiOS supports the use of active/passive HA, similar to that for Amazon Web Services (AWS) in an Azure environment.

New CLI options are available to configure with Azure:

- The `system sdn-connector` contains a connector type for Azure environments called `azure`.
- The `nic` option enables you to configure the Azure network interface.
- The `route-table` option enables you to configure the Azure route table.

#### Example:

```
config system sdn-connector
  edit "azd"
```

```

set type azure
config nic
  edit nic-eth2
    config ip
      edit ipconfig1
        set public-ip p3
      next
    end
  next
  edit nic-eth3
    config ip
      edit ipconfig1
        set public-ip p2
      next
    end
  next
end
config route-table
  edit 1
    config route
      edit 12
        set next-hop 111.233.222.233
      next
    end
  next
end

```

In addition to the options for HA already specified, there are settings specific to Azure connectivity within the `system sdn-connector` context once the `type` has been set to `azure`.

Option	Description
<b>tenant-id</b>	Azure tenant ID (directory ID).
<b>subscription-id</b>	Azure subscription ID.
<b>client-id</b>	Azure client ID (application ID).
<b>client-secret</b>	Azure client secret (application key).
<b>resource-group</b>	Azure resource group.
<b>azure-region</b>	Global/China Azure Region.
<b>update-interval</b>	Dynamic object update interval in seconds (0 - 3600, 0 means disabled, default = 60).

Online documentation can be found at <http://cookbook.fortinet.com/microsoft-azure/>

## Google Cloud Platform (GCP)

The following FortiGate-VM models will be supported on Google Cloud Platform:

- FG-VM01
- FG-VM02
- FG-VM04
- FG-VM08



FG-WM00 is not supported.

Since GCP use netmask 32, static route must be configured on GCP VPC, instead of FGT.

Licenses will be interchangeable between platforms. A FG-VM04 license that functions in a VMware or Citrix environment can be also used in the GCP environment as well.

While an .out file will be necessary for upgrading, full downloadable images will not be needed for initial installation of the solution. GCP consists of preexisting images that can be checked out of their library and deployed instantly. A difference between this environment and enterprise virtualization platforms is that machine size can never change. An n1-standard-4 has exactly 15 GB of RAM and 4 vCPUs. This can never be changed or edited by the end user or administrator.

The currently available GCP instances we are looking to support are as follows (these will/could change as vNIC values reveal themselves):

FG-VM	Equates to Instance Type	vCPU	RAM	Disks
FG-VM01-GC	n1-standard-1	1	3.75GB	16 (32 in Beta)
FG-VM02-GC	n1-standard-2	2	7.50 GB	16 (64 in Beta)
FG-VM04-GC	n1-standard-4	4	15 GB	16 (64 in Beta)
FG-VM08-GC	n1-standard-8	8	30 GB	16 (128 in Beta)
FG-VM16-GC	n1-standard-16	16	60 GB	16 (128 in Beta)
FG-VM32-GC	n1-standard-32	32	88 GB	16 (128 in Beta)
FG-VMUL-GC	any of the above and any new that could be created.			

Additional information from GCP: <https://cloud.google.com/compute/docs/images/building-custom-os>.

## HA support for GCP

FortiOS supports the use of active/passive HA, using a unicast heartbeat, in Google Cloud Platform (GCP) similar to the HA support for Amazon Web Services (AWS).

This support includes:

- HA in the same region within a project
- HA session and configuration synchronization

- Automatic failover to the passive unit (time dependent on configuration), using the built-in API call to GCP for changing the routing path from the active unit to the passive unit.

There is a new connector type, `gcp`, that has been added to the `type` option for `system sdn-connector` as well as a setting for the mask of the unicast heartbeat in `system ha`.

### GCP type example:

```
config system sdn-connector
  edit gcp
    set type gcp
    config external-ip
      edit gundam-public
        next
      end
    config route
      edit gundam-route
        next
      end
    next
  end
```

### Unicast example:

```
config system ha
  set group-id 20
  set group-name "cluster1"
  set mode a-p
  set hbdev "port3" 50
  set ha-mgmt-status enable
  config ha-mgmt-interfaces
    edit 1
      set interface "port4"
      set gateway 172.16.100.1
    next
  end
  set override disable
  set priority 20
  set unicast-hb enable
  set unicast-hb-peerip 172.16.201.3
  set unicast-hb-netmask 255.255.255.0
end
```

## Oracle Cloud Infrastructure (OCI)

### SDN connector support

Support has been added to enable SDN connector support for FortiGate in Oracle Cloud Infrastructure. This connector makes calls to the OCI API to get information about VMs running in the OCI cloud.

The connector is configured by using the commands:

```
config sys sdn
  edit <name of sdn controller>
    set status enable
    set type oci
    set tenant-id <id>
```

```
set user-id <user id>
set compartment-id <compartment id>
set oci-region <OCI server region>
set oci-cert <OCI certificate>
set update-interval <interval time>
set filter <filter argument>
end
```

The following OCI filters are supported:

- vm\_name=<vm name>
- instance\_id=<instance id>
- tag.<key>=<value>
- definedtag.<namespace>.<key>=<value>



The values for the filters can have spaces in them as long as the value is inclosed with quotation marks.

---

### HA support for Oracle Cloud Infrastructure

Oracle Cloud Infrastructure (OCI) supports HA for FortiGate-VM. This support does not apply to OCI-Classical or Oracle Public Cloud (OPC).

OCI supports the use of a secondary IP on the virtual network interface (VNIC). This secondary IP is used as the IP of the FortiGate interface instead of the primary IP address, as well as the next hop in the route. When an HA failover occurs, the secondary IP address on the VNIC is changed from master to slave so that the forwarded traffic can go through the new master.



# Deployment example – VMware

Once you have downloaded the FGT\_VMxx-v5-build0xxx-FORTINET.out.ovf.zip file from <http://support.fortinet.com> and extracted the package contents to a folder on your local computer, you can use the vSphere client to create the virtual machine from the deployment package OVF template.

The following topics are included in this section:

[Open the FortiGate VM OVF file with the vSphere client](#)

[Configure FortiGate VM hardware settings](#)

[Transparent mode VMware configuration](#)

[High availability VMware configuration](#)

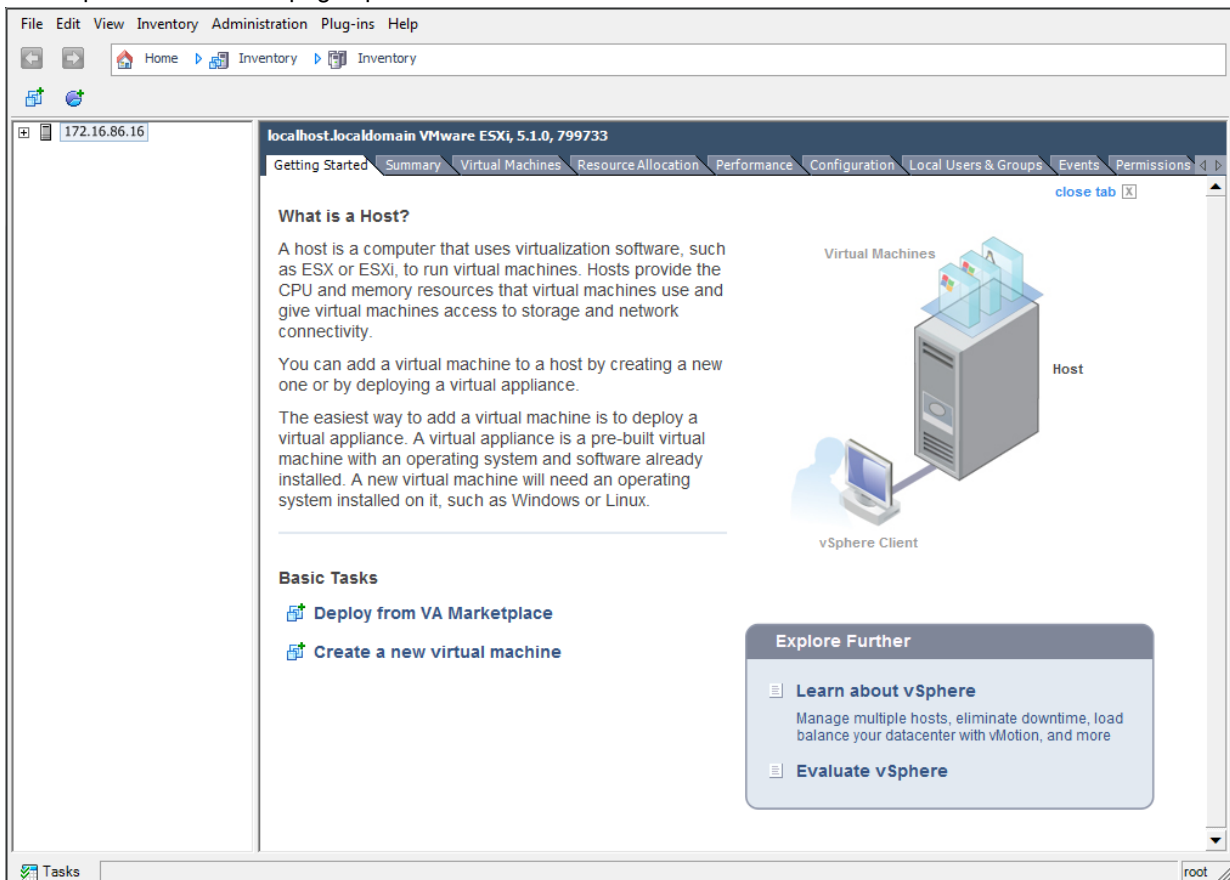
[Power on your FortiGate VM](#)

## Open the FortiGate VM OVF file with the vSphere client

**To deploy the FortiGate VM OVF template:**

1. Launch the VMware vSphere client, enter the IP address or host name of your server, enter your user name and password and select **Login**.

The vSphere client home page opens.



2. Select **File > Deploy OVF Template** to launch the OVF Template wizard.

The OVF Template **Source** page opens.

3. Select the source location of the OVF file. Select **Browse** and locate the OVF file on your computer. Select **Next** to continue.

The OVF Template **Details** page opens.

**OVF Template Details**  
Verify OVF template details.

[Source](#)

**OVF Template Details**  
End User License Agreement  
Name and Location  
Disk Format  
Network Mapping  
Ready to Complete

Product:	Fortigate-VM
Version:	
Vendor:	
Publisher:	No certificate present
Download size:	30.4 MB
Size on disk:	Unknown (thin provisioned) 32.0 GB (thick provisioned)
Description:	FortiGate Virtual Appliance by Fortinet Technologies Inc. ( <a href="http://www.fortinet.com">http://www.fortinet.com</a> )

Help < Back Next > Cancel

4. Verify the OVF template details. This page details the product name, download size, size on disk, and description. Select **Next** to continue.

The OVF Template **End User License Agreement** page opens.

**End User License Agreement**  
Accept the end user license agreements.

[Source](#)  
[OVF Template Details](#)  
**End User License Agreement**  
Name and Location  
Disk Format  
Network Mapping  
Ready to Complete

End User License Agreement for FortiGate Virtual Appliance

NOTICE TO ALL USERS: PLEASE READ THE TERMS AND CONDITIONS OF THE LICENSE AGREEMENT CAREFULLY. FORTINET, INC. IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN CONTRACT SIGNED BY YOU. IF YOU DO NOT AGREE, CLICK ON THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS LICENSE AGREEMENT AND DO NOT INSTALL THE SOFTWARE. IF YOU PURCHASED THE SOFTWARE ON TANGIBLE MEDIA (e.g., CD) WITHOUT THE OPPORTUNITY TO REVIEW THIS LICENSE AND YOU DO NOT ACCEPT THIS LICENSE AGREEMENT, YOU MAY OBTAIN A REFUND OF THE AMOUNT YOU ORIGINALLY PAID IF YOU: (A) DO NOT USE THE SOFTWARE AND (B) RETURN IT, WITH PROOF OF PAYMENT, WITHIN THIRTY (30) DAYS OF THE PURCHASE DATE TO THE LOCATION FROM WHICH IT WAS OBTAINED.

This End User License Agreement (EULA) is an agreement between you and Fortinet, Inc. ("Fortinet"), which governs your use of this software product. A software license and a license key or "unlock code" ("Software License"), issued to a designated user only by Fortinet or its authorized agents, is required for each computer on which the Software is loaded.

Definitions: (a) "Software" means (a) all means (a) all of the contents of the files, disk(s), CD-ROM(s) or other media (including electronic media) with which this Agreement is provided or such contents as are hosted by Fortinet or its distributors, resellers, OEM/MSP partners, or other business partners (collectively "Authorized Partner(s)"), including but not limited to (i) Fortinet or third party computer information or software; (ii) related explanatory materials in printed, electronic, or online form ("Documentation"); and (b) upgrades, modified or subsequent versions and updates (collectively "Updates"), and Software, if any, licensed to you by Fortinet or an

Accept

Help < Back Next > Cancel

5. Read the end user license agreement for FortiGate VM. Select **Accept** and then select **Next** to continue.

The OVF Template **Name and Location** page opens.

**Name and Location**  
Specify a name and location for the deployed template

[Source](#)  
[OVF Template Details](#)  
[End User License Agreement](#)  
**Name and Location**  
[Disk Format](#)  
[Network Mapping](#)  
[Ready to Complete](#)

Name:  
Fortigate-VM-01  
The name can contain up to 80 characters and it must be unique within the inventory folder.

Help      < Back      Next >      Cancel

6. Enter a name for this OVF template. The name can contain up to 80 characters and it must be unique within the inventory folder. Select **Next** to continue.

The OVF Template **Disk Format** page opens.

**Disk Format**  
In which format do you want to store the virtual disks?

Source  
OVF Template Details  
End User License Agreement  
Name and Location  
**Disk Format**  
Network Mapping  
Ready to Complete

Datastore: datastore 1

Available space (GB): 394.6

☒ Thick Provision Lazy Zeroed  
☐ Thick Provision Eager Zeroed  
☐ Thin Provision

Help < Back Next > Cancel

7. Select one of the following:
  - **Thick Provision Lazy Zeroed:** Allocates the disk space statically (no other volumes can take the space), but does not write zeros to the blocks until the first write takes place to that block during runtime (which includes a full disk format).
  - **Thick Provision Eager Zeroed:** Allocates the disk space statically (no other volumes can take the space), and writes zeros to all the blocks.
  - **Thin Provision:** Allocates the disk space only when a write occurs to a block, but the total volume size is reported by VMFS to the OS. Other volumes can take the remaining space. This allows you to float space between your servers, and expand your storage when your size monitoring indicates there is a problem. Note that once a Thin Provisioned block is allocated, it remains on the volume regardless if you have deleted data, etc.
8. Select **Next** to continue.

The OVF Template **Network Mapping** page opens.

**Network Mapping**  
What networks should the deployed template use?

[Source](#)  
[OVF Template Details](#)  
[End User License Agreement](#)  
[Name and Location](#)  
[Disk Format](#)  
**Network Mapping**  
Ready to Complete

Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
Network 1	VM Network
Network 2	VM Network
Network 3	VM Network
Network 4	VM Network
Network 5	VM Network
Network 6	VM Network
Network 7	VM Network

Description:  
The VM Network network

Warning: Multiple source networks are mapped to the host network: VM Network

[Help](#) [< Back](#) [Next >](#) [Cancel](#)

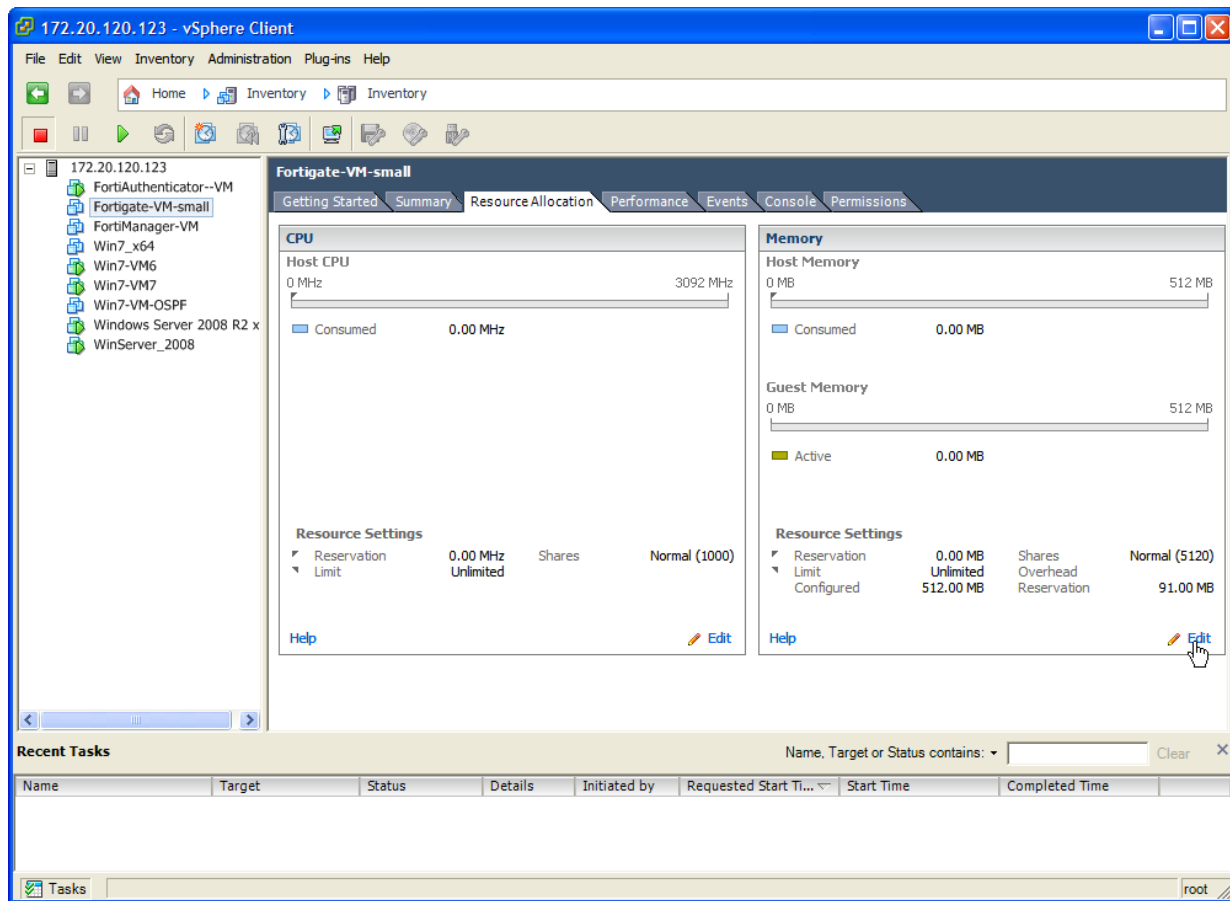
- Map the networks used in this OVF template to networks in your inventory. Network 1 maps to port1 of the FortiGate VM. You must set the destination network for this entry to access the device console. Select **Next** to continue.

The OVF Template **Ready to Complete** page opens.

- Review the template configuration. Make sure that **Power on after deployment** is not enabled. You might need to configure the FortiGate VM hardware settings prior to powering on the FortiGate VM.
- Select **Finish** to deploy the OVF template. You will receive a **Deployment Completed Successfully** dialog box once the FortiGate VM OVF template wizard has finished.

## Configure FortiGate VM hardware settings

Before powering on your FortiGate VM you must configure the virtual memory, virtual CPU, and virtual disk configuration to match your FortiGate VM license.



## Transparent mode VMware configuration

If you want to use your FortiGate-VM in transparent mode, your VMware server's virtual switches must operate in promiscuous mode. This permits these interfaces to receive traffic that will pass through the FortiGate unit but was not addressed to the FortiGate unit.

In VMware, promiscuous mode must be explicitly enabled:

1. In the vSphere client, select your VMware server in the left pane and then select the **Configuration** tab in the right pane.
2. In **Hardware**, select **Networking**.
3. Select **Properties** of vSwitch0.
4. In the **Properties** window left pane, select **vSwitch** and then select **Edit**.
5. Select the **Security** tab, set **Promiscuous Mode** to **Accept**, then select **OK**.
6. Select **Close**.
7. Repeat steps 3 through 6 for other vSwitches that your transparent mode FortiGate-VM uses.



## High availability VMware configuration

If you want to combine two or more FortiGate-VM instances into a FortiGate Clustering Protocol (FGCP) High Availability (HA) cluster the VMware server's virtual switches used to connect the heartbeat interfaces must operate in promiscuous mode. This permits HA heartbeat communication between the heartbeat interfaces. HA heartbeat packets are non-TCP packets that use Ethertype values 0x8890, 0x8891, and 0x8890. The FGCP uses link-local IPv4 addresses in the 169.254.0.x range for HA heartbeat interface IP addresses.

To enable promiscuous mode in VMware:

1. In the vSphere client, select your VMware server in the left pane and then select the **Configuration** tab in the right pane.
2. In **Hardware**, select **Networking**.
3. Select **Properties** of a virtual switch used to connect heartbeat interfaces.
4. In the **Properties** window left pane, select **vSwitch** and then select **Edit**.
5. Select the **Security** tab, set **Promiscuous Mode** to **Accept**, then select **OK**.
6. Select **Close**.

You must also set the virtual switches connected to other FortiGate interfaces to allow MAC address changes and to accept forged transmits. This is required because the FGCP sets virtual MAC addresses for all FortiGate interfaces and the same interfaces on the different VM instances in the cluster will have the same virtual MAC addresses.

To make the required changes in VMware:

1. In the vSphere client, select your VMware server in the left pane and then select the **Configuration** tab in the right pane.
2. In **Hardware**, select **Networking**.
3. Select **Properties** of a virtual switch used to connect FortiGate VM interfaces.
4. Set **MAC Address Changes** to **Accept**.
5. Set **Forged Transmits** to **Accept**.

## Power on your FortiGate VM

You can now proceed to power on your FortiGate VM. There are several ways to do this:

- Select the name of the FortiGate VM you deployed in the inventory list and select **Power on the virtual machine** in the **Getting Started** tab.
- In the inventory list, right-click the name of the FortiGate VM you deployed, and select **Power > Power On**.
- Select the name of the FortiGate VM you deployed in the inventory list. Click the **Power On** button on the toolbar.

Select the Console tab to view the console. To enter text, you must click in the console pane. The mouse is then captured and cannot leave the console screen. As the FortiGate console is text-only, no mouse pointer is visible. To release the mouse, press Ctrl-Alt.

# Deployment example – MS Hyper-V

Once you have downloaded the FGT\_VMxx\_HV-v5-build0xxx-FORTINET.out.hyperv.zip file and extracted the package contents to a folder on your Microsoft server, you can deploy the VHD package to your Microsoft Hyper-V environment.

The following topics are included in this section:

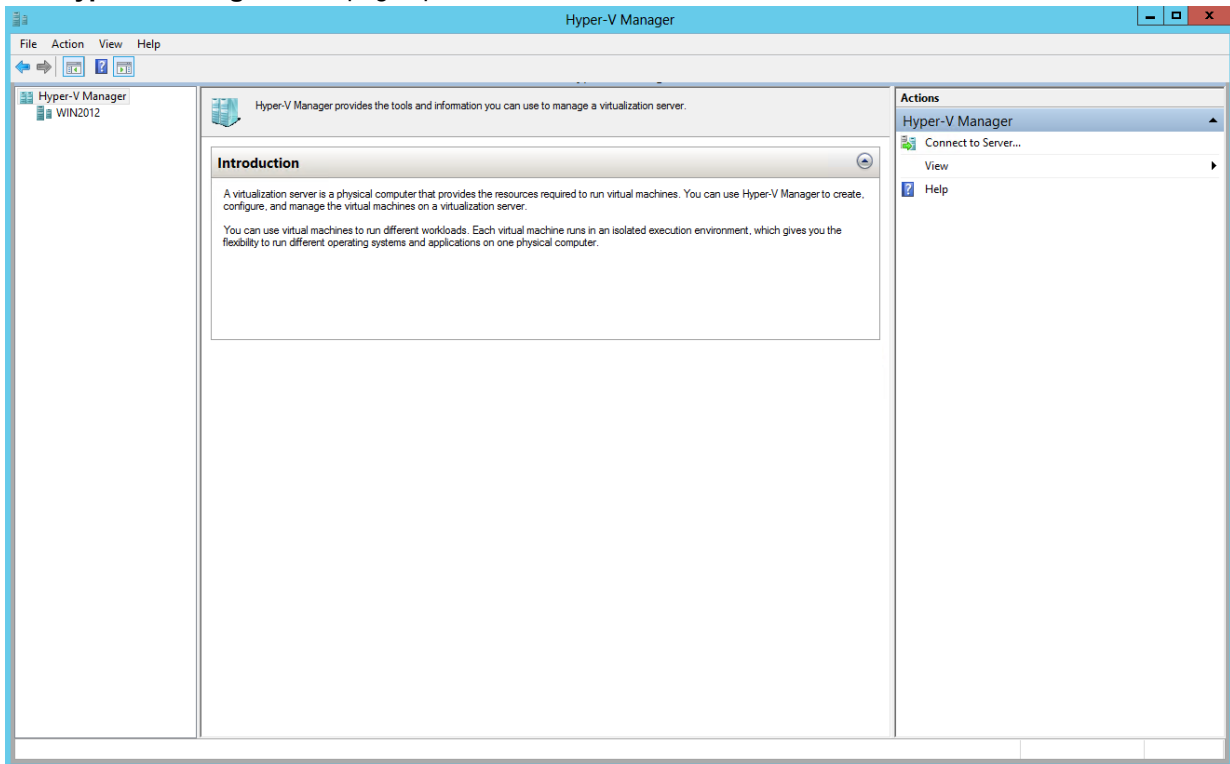
- Create the FortiGate VM virtual machine
- Configure FortiGate VM hardware settings
- High availability Hyper-V configuration
- Start the FortiGate VM

## Create the FortiGate VM virtual machine

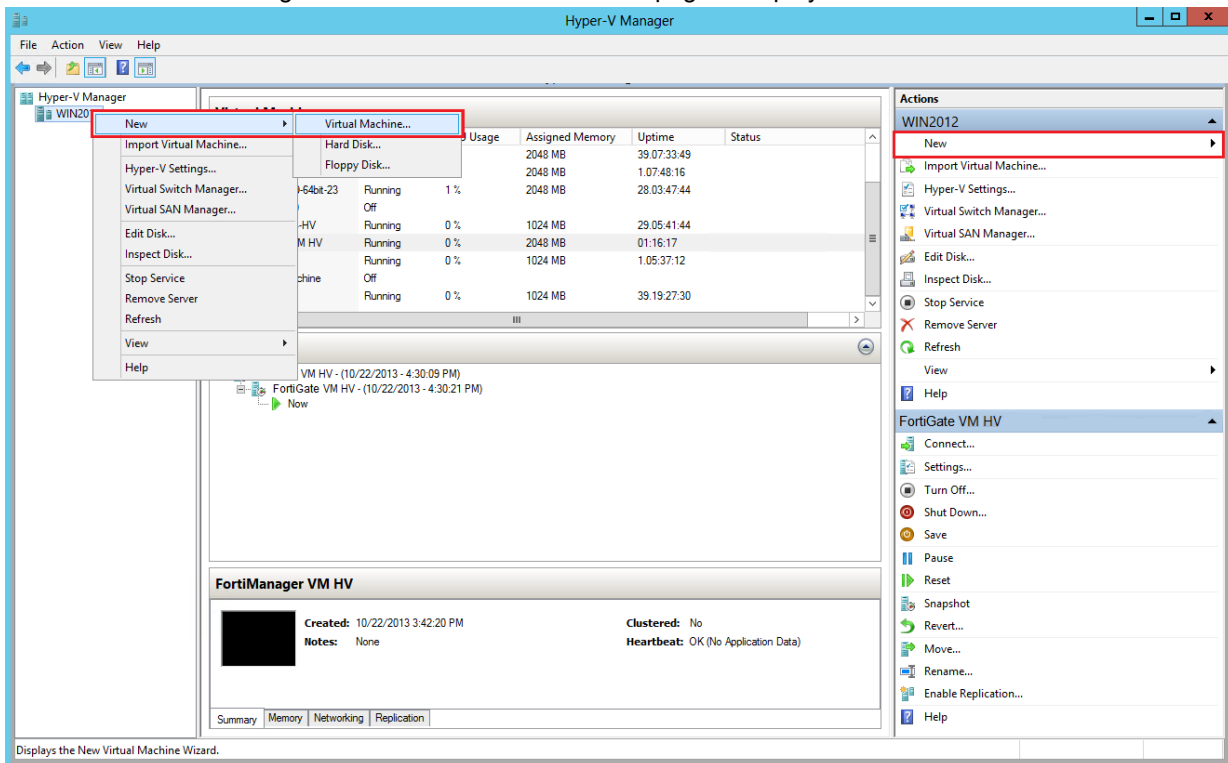
To create the FortiGate VM virtual machine:

1. Launch the Hyper-V Manager in your Microsoft server.

The **Hyper-V Manager** home page opens.

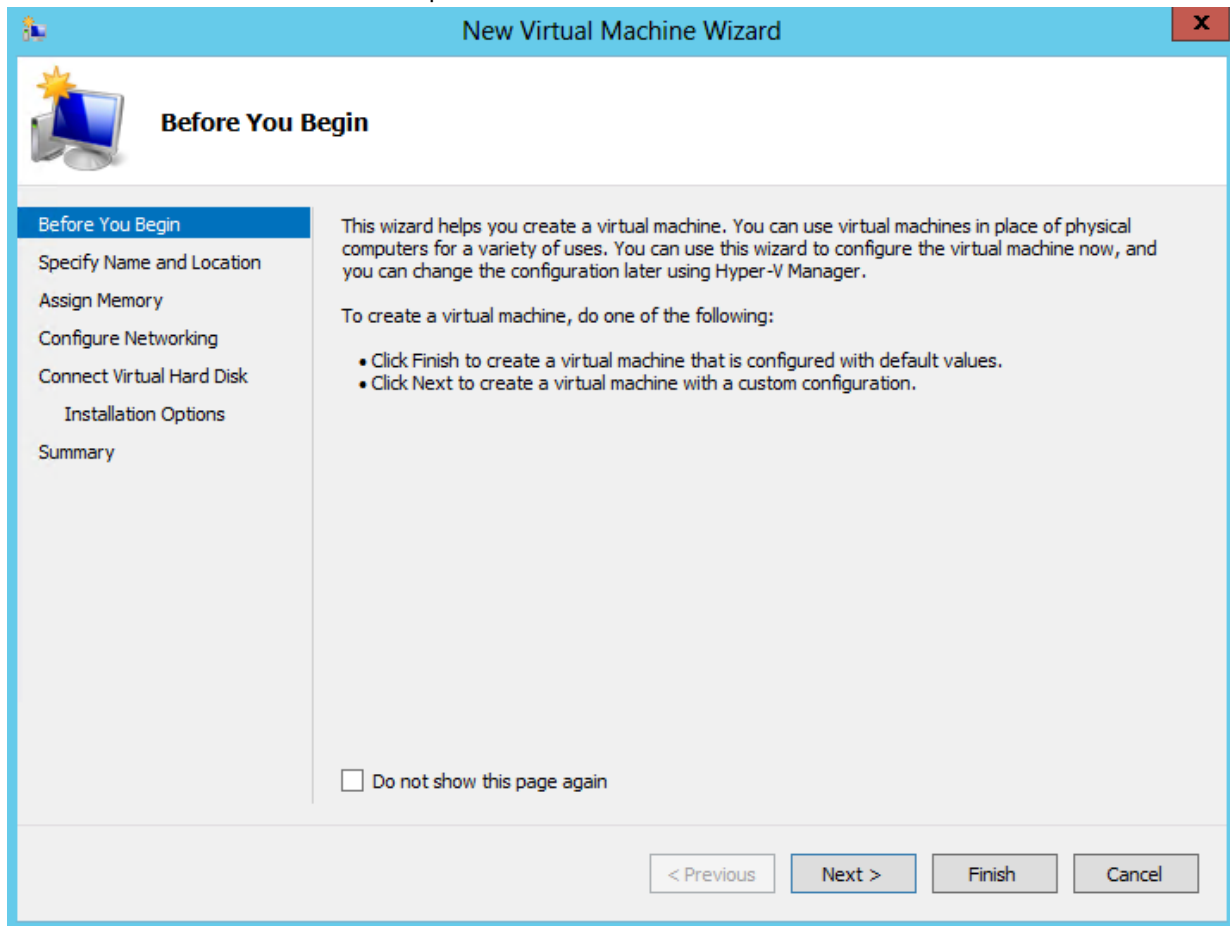


2. Select the server in the right-tree menu. The server details page is displayed.



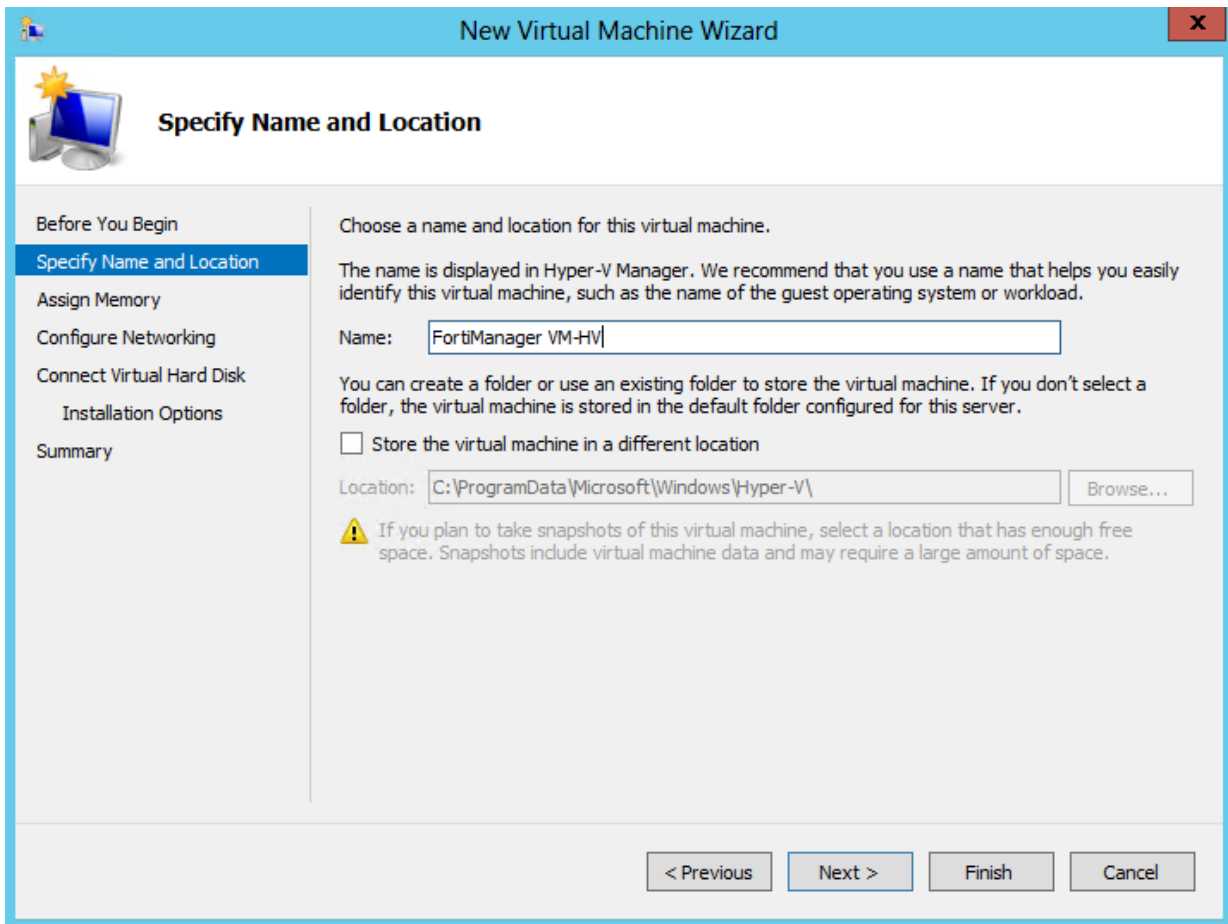
3. Right-click the server and select **New** and select **Virtual Machine** from the menu. Optionally, in the **Actions** menu, select **New** and select **Virtual Machine** from the menu.

The **New Virtual Machine Wizard** opens.



4. Select **Next** to create a virtual machine with a custom configuration.

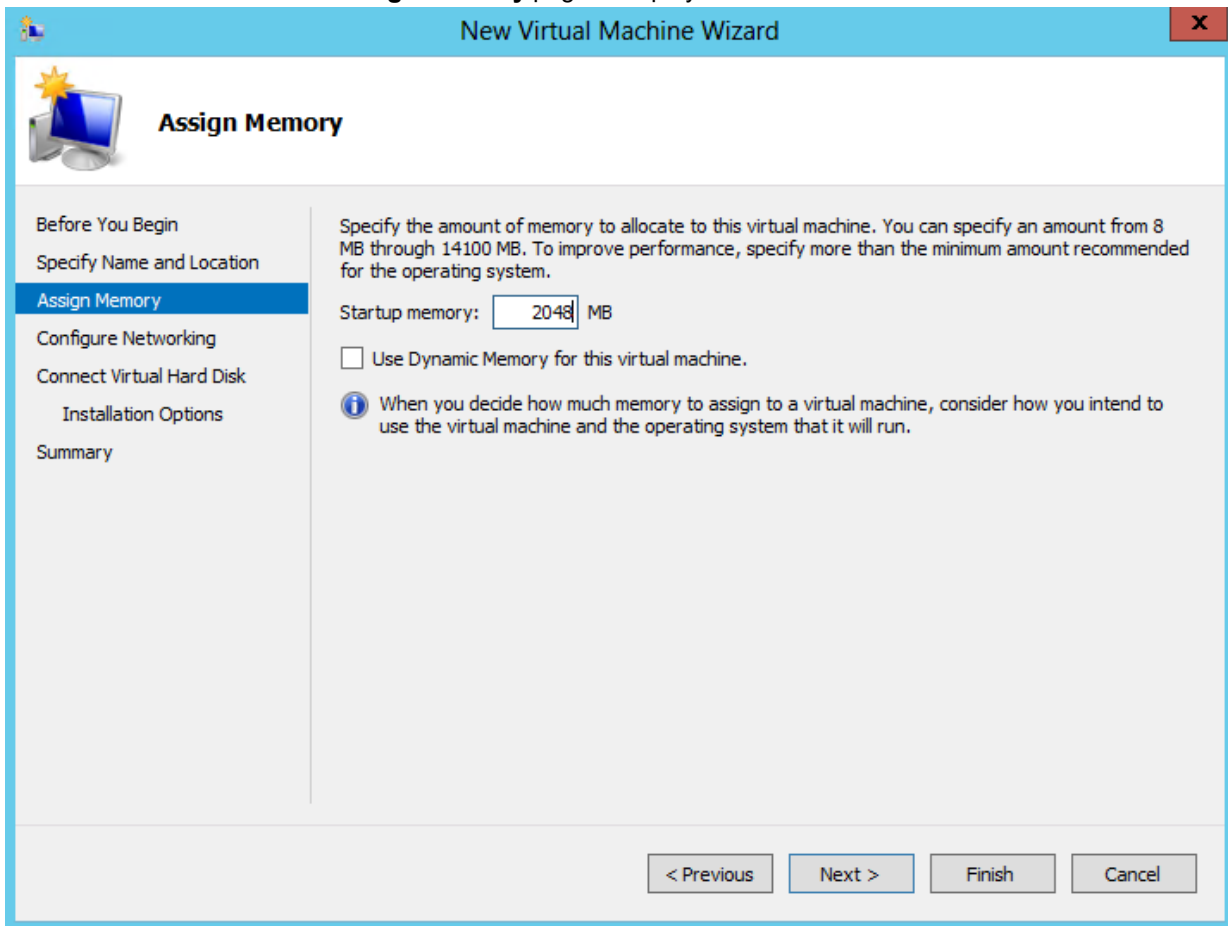
The **Specify Name and Location** page is displayed.



The screenshot shows the 'New Virtual Machine Wizard' window with the title bar 'New Virtual Machine Wizard' and a close button. The main window has a blue header bar with the title 'Specify Name and Location' and a small icon of a computer with a star. On the left, there is a navigation pane with the following steps: 'Before You Begin', 'Specify Name and Location' (highlighted), 'Assign Memory', 'Configure Networking', 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. The main area contains the following text: 'Choose a name and location for this virtual machine.' followed by 'The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.' Below this is a 'Name:' label and a text box containing 'FortiManager VM-HV'. Then, 'You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.' followed by an unchecked checkbox 'Store the virtual machine in a different location'. Below that is a 'Location:' label and a text box containing 'C:\ProgramData\Microsoft\Windows\Hyper-V\' with a 'Browse...' button to its right. At the bottom of the main area is a warning icon and text: 'If you plan to take snapshots of this virtual machine, select a location that has enough free space. Snapshots include virtual machine data and may require a large amount of space.' At the bottom of the window are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

5. Enter a name for this virtual machine. The name is displayed in the Hyper-V Manager.

Select **Next** to continue. The **Assign Memory** page is displayed.



**New Virtual Machine Wizard**


**Assign Memory**

Before You Begin  
Specify Name and Location  
**Assign Memory**  
Configure Networking  
Connect Virtual Hard Disk  
Installation Options  
Summary

Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 8 MB through 14100 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory:  MB

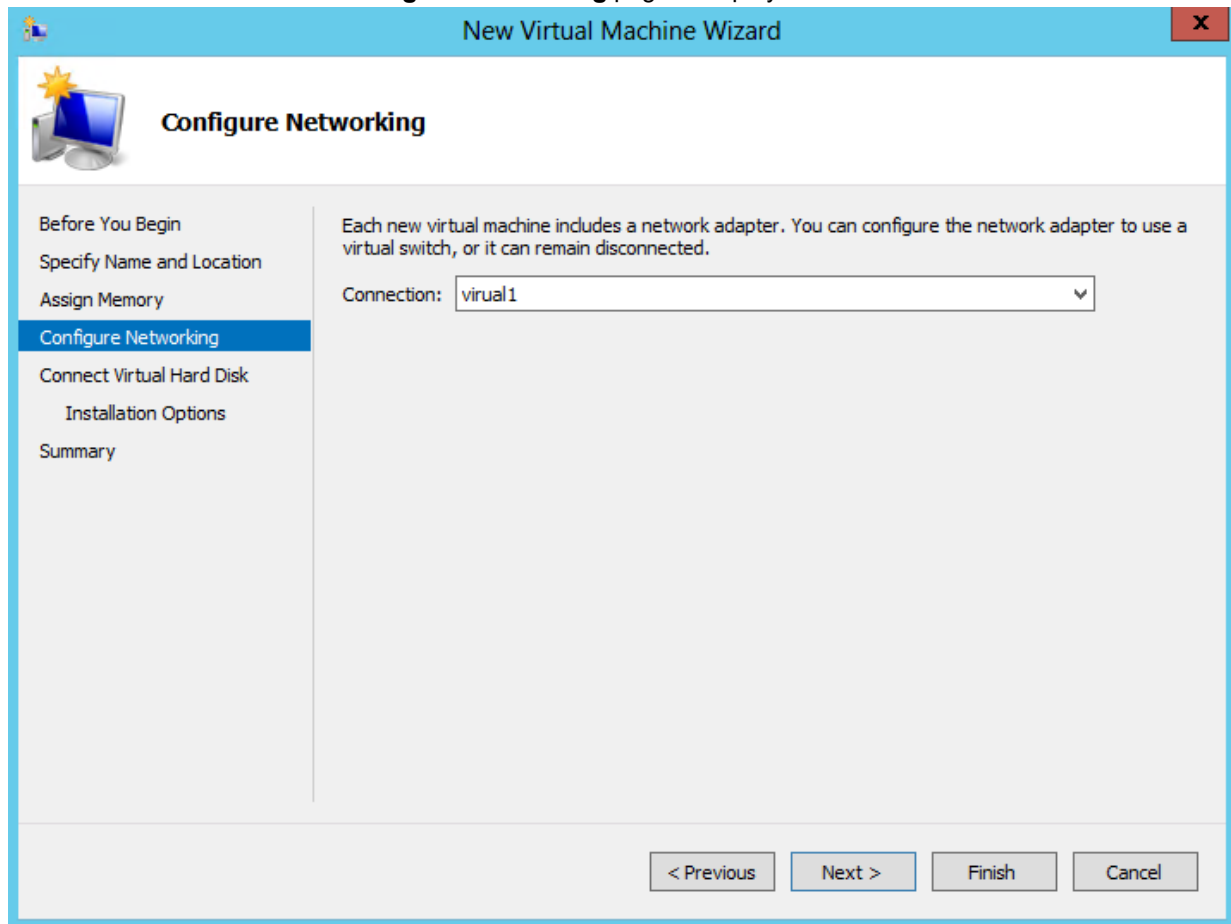
☐ Use Dynamic Memory for this virtual machine.

 When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

< Previous   Next >   Finish   Cancel

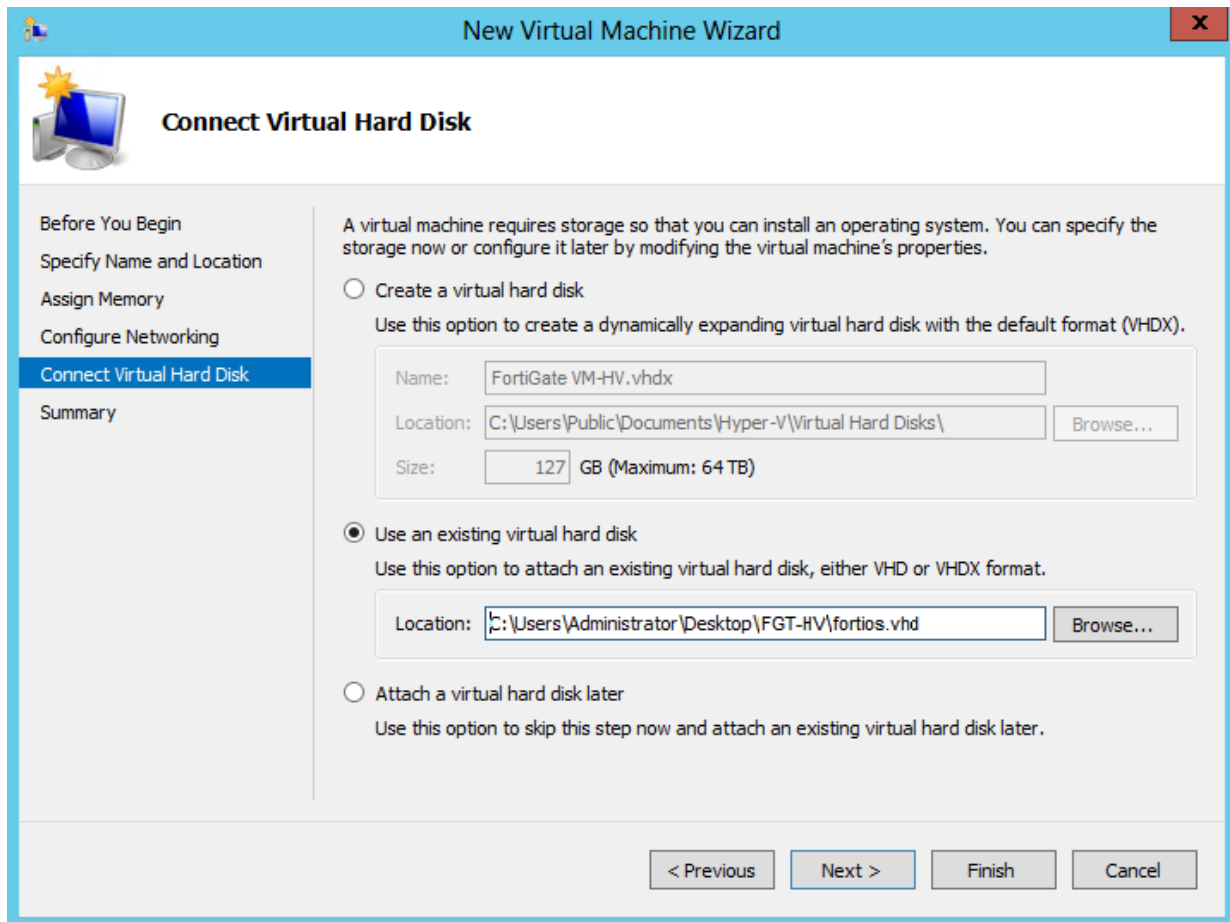
- Specify the amount of memory to allocate to this virtual machine. The default memory for FortiGate VM is 1GB (1024MB).

Select **Next** to continue. The **Configure Networking** page is displayed.



- Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected. FortiGate VM requires four network adapters. You must configure network adapters in the **Settings** page.

Select **Next** to continue. The **Connect Virtual Hard Disk** page is displayed.



The screenshot shows the 'New Virtual Machine Wizard' window with the 'Connect Virtual Hard Disk' step selected in the left-hand navigation pane. The main area contains instructions and three options for connecting a virtual hard disk. The first option, 'Create a virtual hard disk', is unselected. The second option, 'Use an existing virtual hard disk', is selected with a radio button. The third option, 'Attach a virtual hard disk later', is unselected. The 'Location' field for the selected option contains the path 'C:\Users\Administrator\Desktop\FGT-HV\fortios.vhd'. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

**New Virtual Machine Wizard**

**Connect Virtual Hard Disk**

Before You Begin  
Specify Name and Location  
Assign Memory  
Configure Networking  
**Connect Virtual Hard Disk**  
Summary

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

☐ Create a virtual hard disk  
Use this option to create a dynamically expanding virtual hard disk with the default format (VHDX).

Name: FortiGate VM-HV.vhdx  
Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ Browse...  
Size: 127 GB (Maximum: 64 TB)

☒ Use an existing virtual hard disk  
Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

Location: C:\Users\Administrator\Desktop\FGT-HV\fortios.vhd Browse...

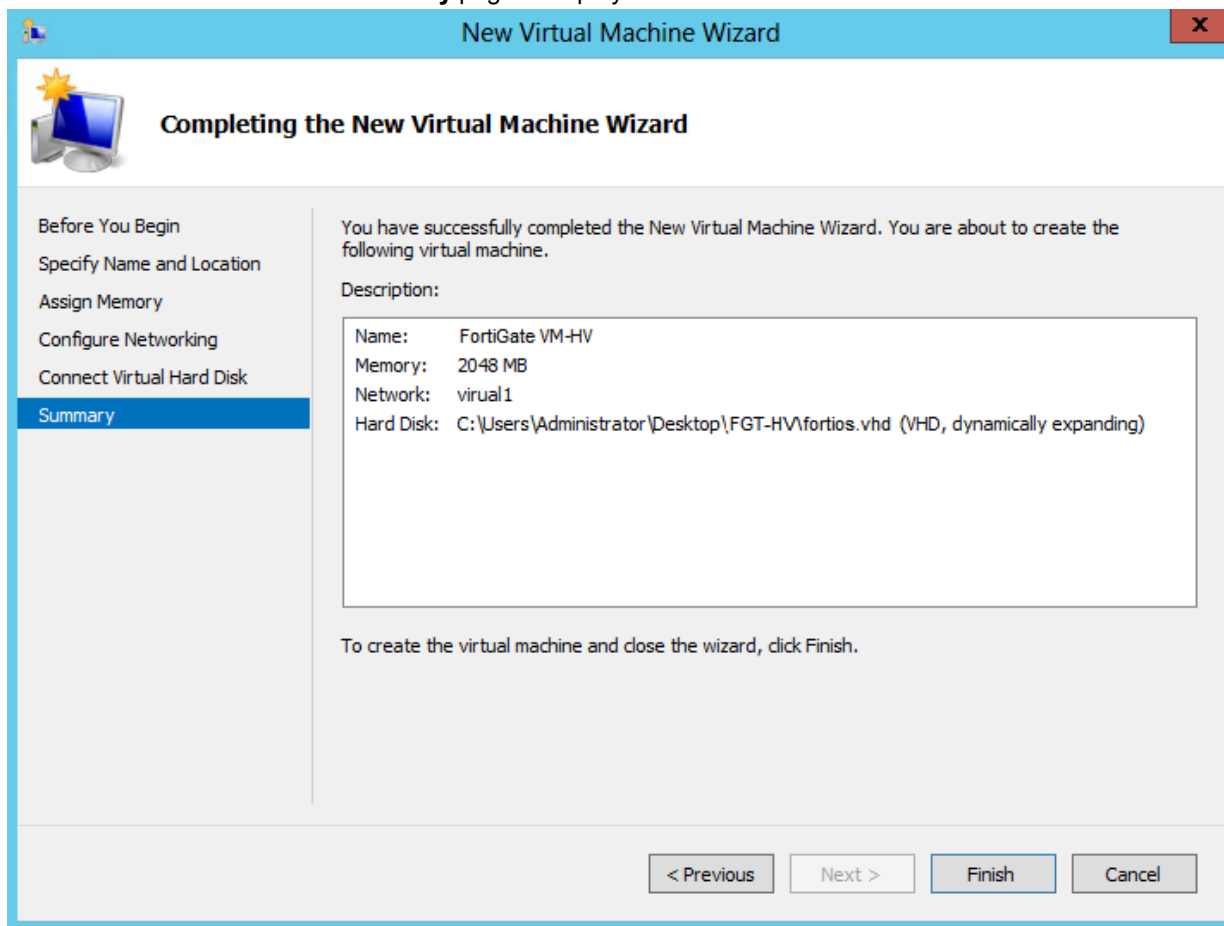
☐ Attach a virtual hard disk later  
Use this option to skip this step now and attach an existing virtual hard disk later.

< Previous Next > Finish Cancel

8. Select to use an existing virtual hard disk and browse for the `fortios.vhd` file that you downloaded from the [Fortinet Customer Service & Support portal](#).



Select **Next** to continue. The **Summary** page is displayed.



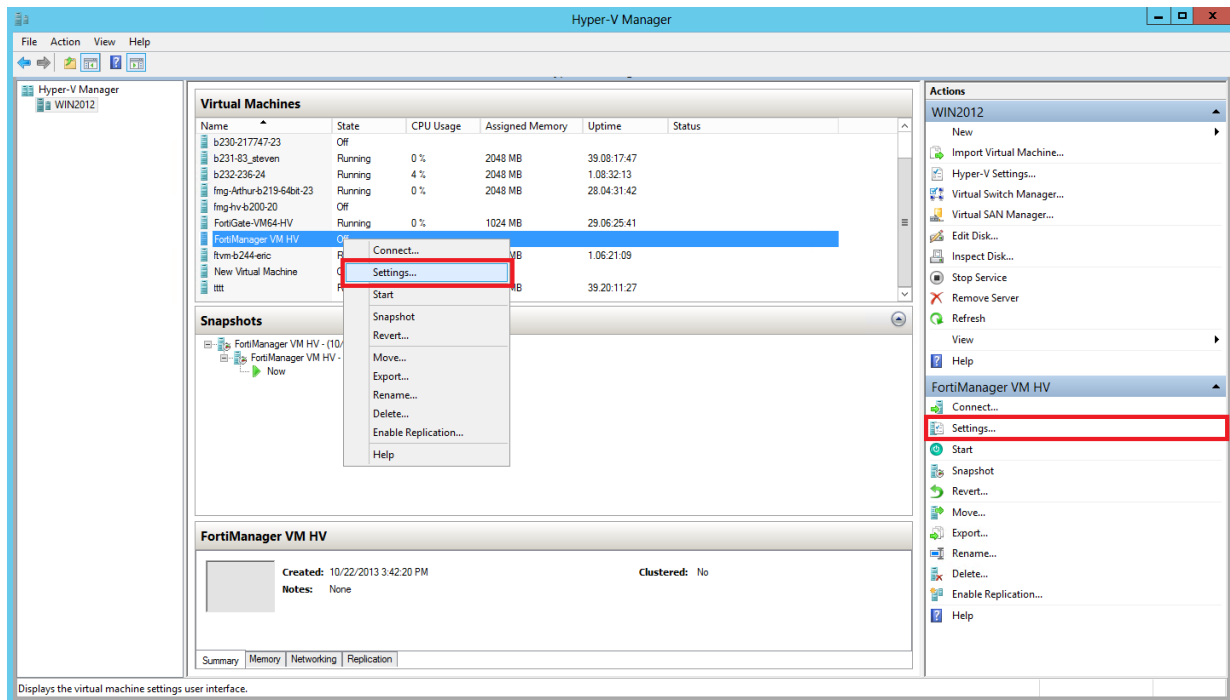
9. To create the virtual machine and close the wizard, select **Finish**.

## Configure FortiGate VM hardware settings

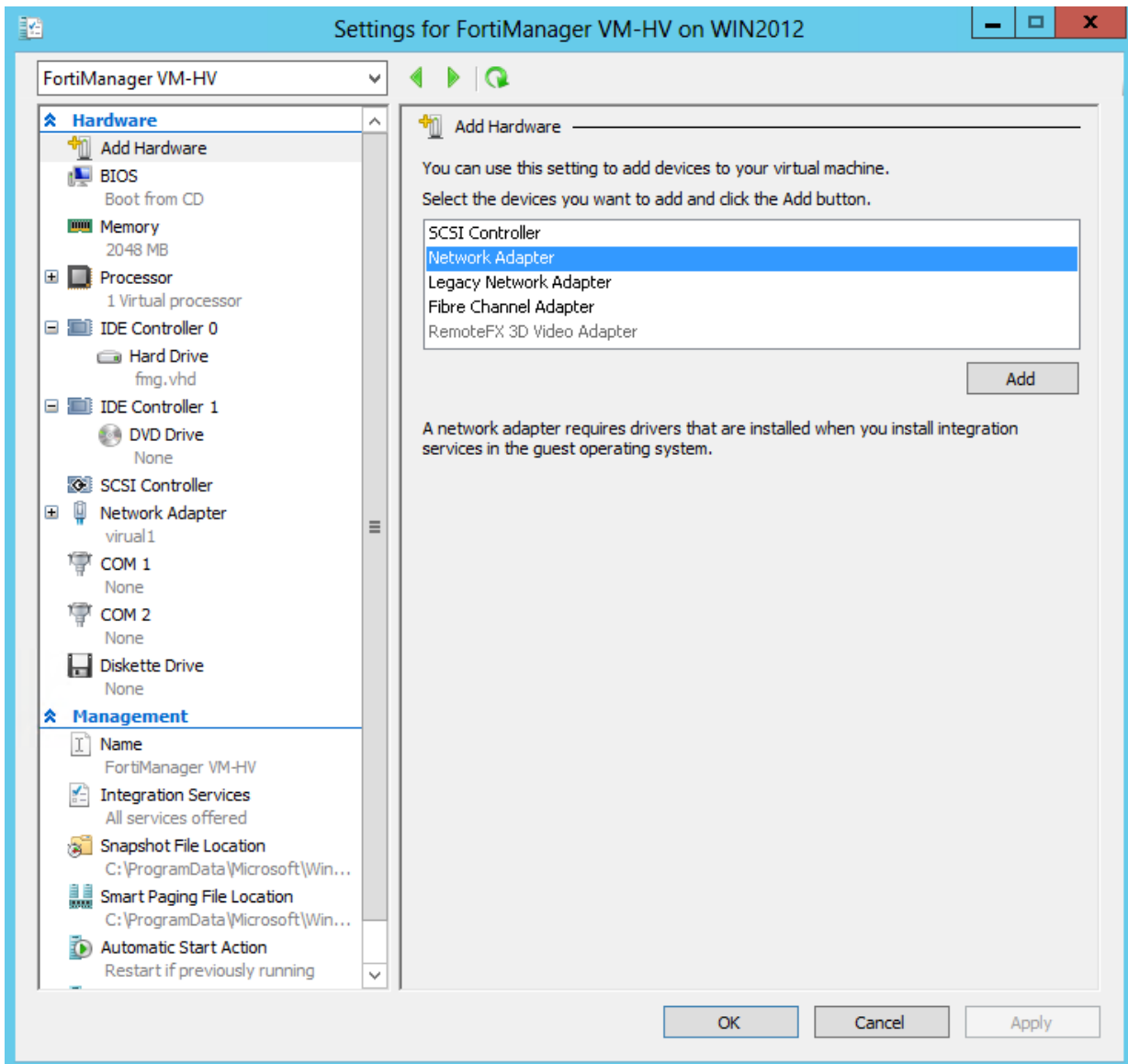
Before powering on your FortiGate VM you must configure the virtual memory, virtual CPU, and virtual disk configuration to match your FortiGate VM license.

### To configure settings for FortiGate VM on the server:

1. In the Hyper-V Manager, locate the name of the virtual machine, right-click the entry, and select **Settings** from the menu. Optionally, you can select the virtual machine and select **Settings** in the **Actions** menu.



The **Settings** page is displayed.



2. Configure virtual processors, network adapters, and virtual hard drive settings.
3. Select **Apply** to save the settings and then select **OK** to close the settings page.

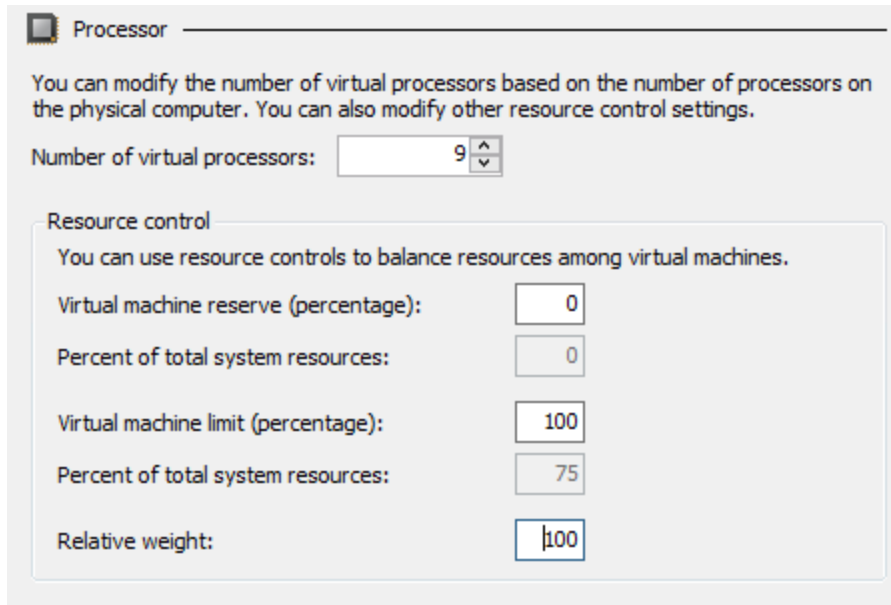
## FortiGate VM virtual processors

You must configure FortiGate VM virtual processors in the server settings page. The number of processors is dependent on your server environment.

### Configure FortiGate VM virtual processors:

1. In the **Settings** page, select **Processor** from the **Hardware** menu.

The **Processor** page is displayed.



**Processor**

You can modify the number of virtual processors based on the number of processors on the physical computer. You can also modify other resource control settings.

Number of virtual processors:

**Resource control**

You can use resource controls to balance resources among virtual machines.

Virtual machine reserve (percentage):

Percent of total system resources:

Virtual machine limit (percentage):

Percent of total system resources:

Relative weight:

2. Configure the number of virtual processors for the FortiGate VM virtual machine. Optionally, you can use resource controls to balance resources among virtual machines.
3. Select **Apply** to save the settings.

## FortiGate VM network adapters

You must configure FortiGate VM network adapters in the server settings page. FortiGate VM supports four network adapters.

### Configure FortiGate VM network adapters:

1. In the **Settings** page, select **Add Hardware** from the **Hardware** menu, select **Network Adapter** in the device list, and select the **Add** button.

The **Network Adapter** page is displayed.

The screenshot shows the 'Network Adapter' configuration page. At the top, it says 'Specify the configuration of the network adapter or remove the network adapter.' Below this, there is a 'Virtual switch:' dropdown menu with 'Broadcom NetXtreme Gigabit Ethernet - Virtual Switch' selected. Under the 'VLAN ID' section, there is a checkbox 'Enable virtual LAN identification' which is unchecked. Below the checkbox, a text box contains the value '2'. The 'Bandwidth Management' section also has an unchecked checkbox 'Enable bandwidth management'. Below this, there are two rows for 'Minimum bandwidth:' and 'Maximum bandwidth:', each with a text box containing '0' and the unit 'Mbps'. A note at the bottom of this section says 'To leave the minimum or maximum unrestricted, specify 0 as the value.' At the bottom of the page, there is a 'Remove' button and a note: 'To remove the network adapter from this virtual machine, click Remove.' A final note at the very bottom says 'Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.'

1. You must manually configure four network adapters for FortiGate VM in the settings page. For each network adapter, select the virtual switch from the drop-down list.
2. Select **Apply** to save the settings.

## FortiGate VM virtual hard disk


You must configure the FortiGate VM virtual hard disk in the server settings page.

If you know your environment will expand in the future, it is recommended to increase the hard disk size beyond 30GB. The VM license limit is 2TB.

### Configure a FortiGate VM virtual hard drive:

1. In the **Settings** page, select **IDE Controller 0 > Hard Drive** from the **Hardware** menu.

The **Hard Drive** page is displayed.

 **Hard Drive**

You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.


Controller:  Location:

**Media**

You can compact or convert a virtual hard disk by editing the associated file. Specify the full path to the file.

☒ Virtual hard disk:

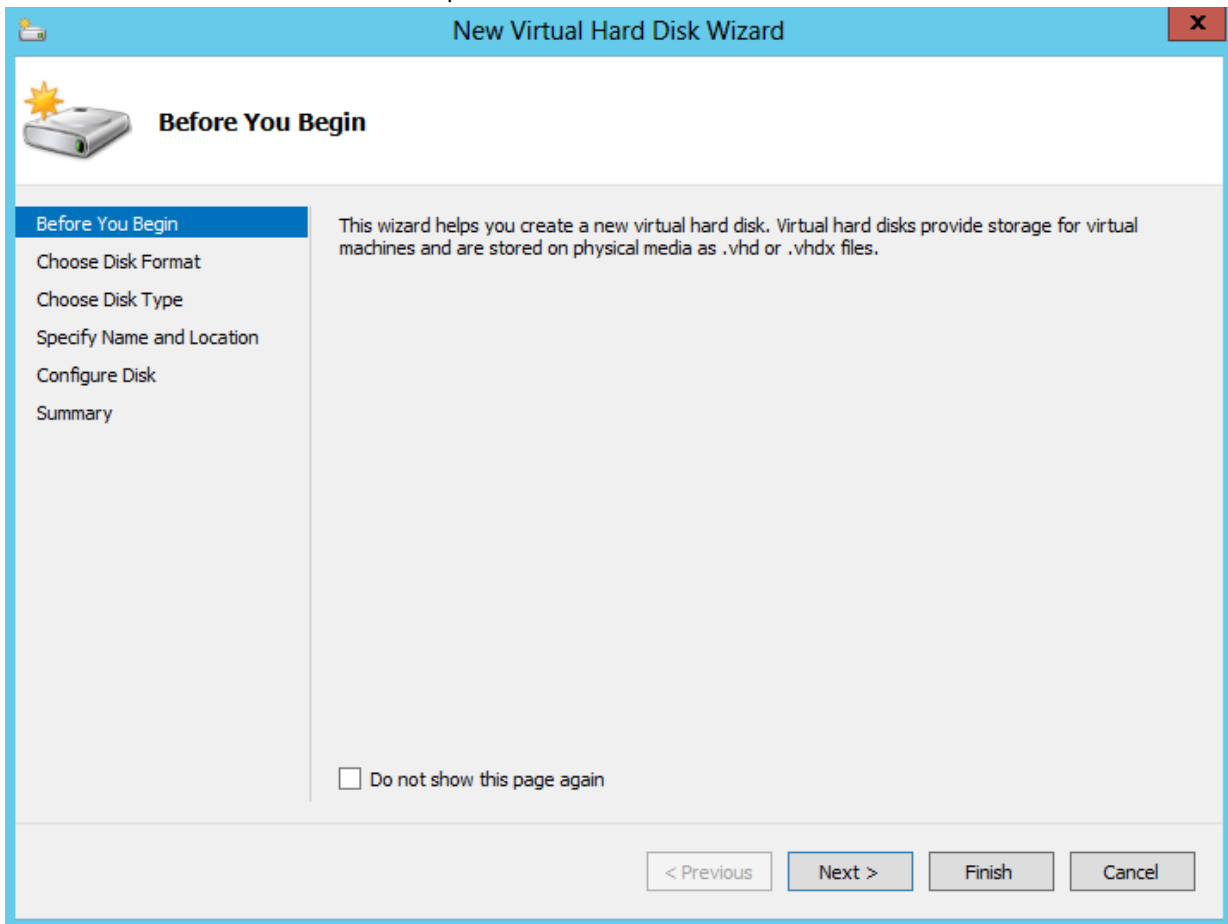
☐ Physical hard disk:

 If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.

To remove the virtual hard disk, click Remove. This disconnects the disk but does not delete the associated file.

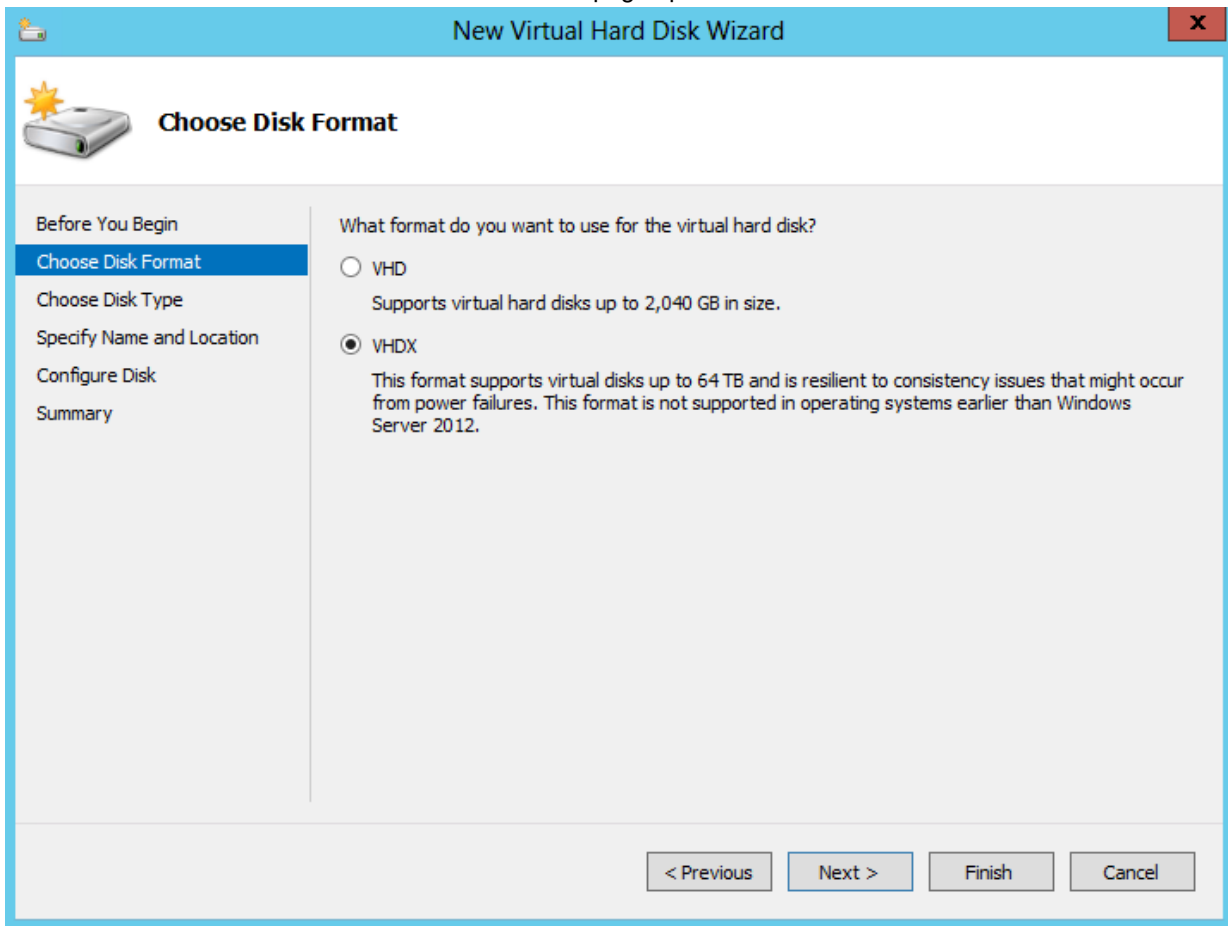
2. Select **New** to create a new virtual hard disk.

The **New Virtual Hard Disk Wizard** opens.



3. This wizard helps you to create a new virtual hard disk.

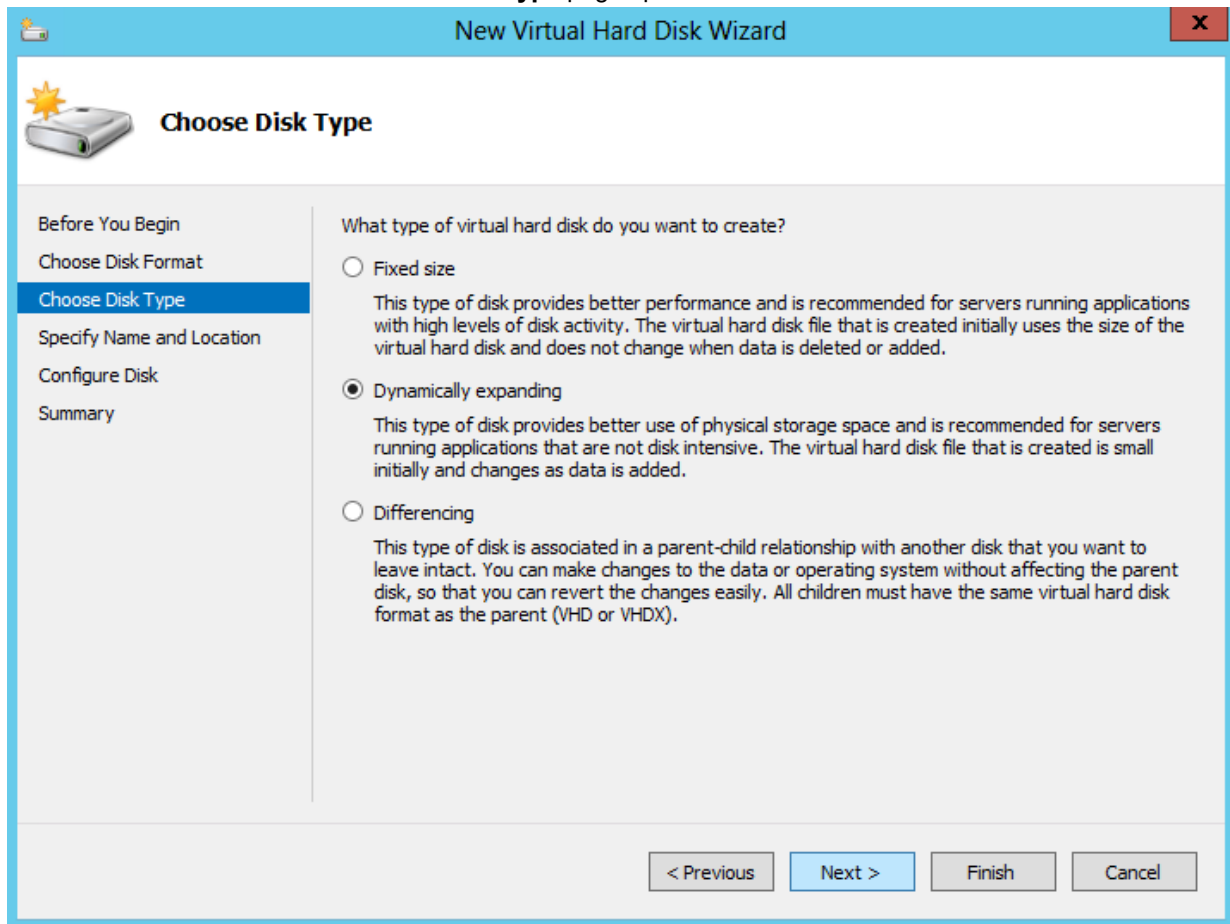
Select **Next** to continue. The **Choose Disk Format** page opens.



4. Select to use VHDX format virtual hard disks. This format supports virtual disks up to 64TB and is resilient to consistency issues that might occur from power failures. This format is not supported in operating systems earlier than Windows Server 2012. Note that FortiGate-VM does not support hard disks larger than 2TB.

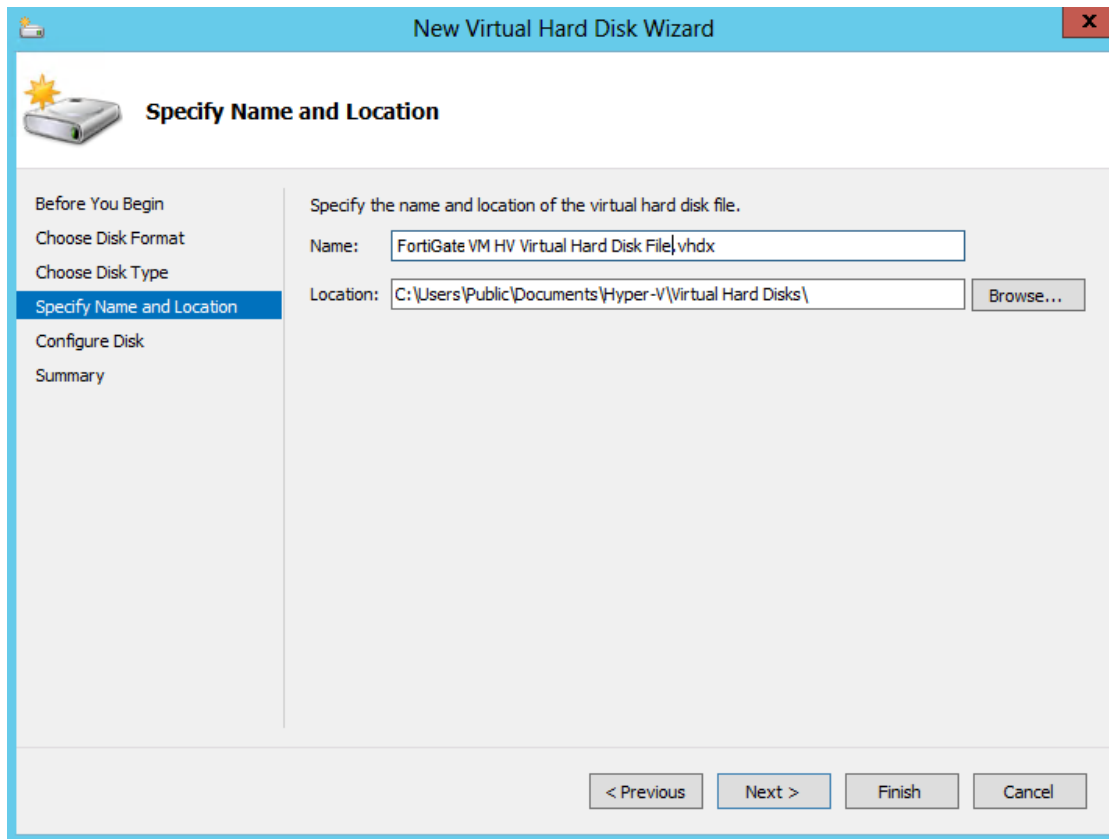


Select **Next** to continue. The **Choose Disk Type** page opens.



5. Select the type of virtual disk you want to use. Select one of the following disk types:
- **Fixed size:** This type of disk provides better performance and is recommended for servers running applications with high levels of disk activity. The virtual hard disk file that is created initially uses the size of the virtual hard disk and does not change when data is deleted or added.
  - **Dynamic expanding:** This type of disk provides better use of physical storage space and is recommended for servers running applications that are not disk intensive. The virtual disk file that is created is small initially and changes as data is added.
  - **Differencing:** This type of disk is associated in a parent-child relationship with another disk that you want to leave intact. You can make changes to the data or operating system without affecting the parent disk, so that you can revert the changes easily. All children must have the same virtual hard disk format as the parent (VHD or VHDX).

Select **Next** to continue. The **Specify Name and Location** page opens.



6. Specify the name and location of the virtual hard disk file. Use the **Browse** button to select a specific file folder on your server.

Select **Next** to continue. The **Configure Disk** page opens.

The screenshot shows the 'New Virtual Hard Disk Wizard' window with the 'Configure Disk' step selected. The left sidebar contains the following steps: 'Before You Begin', 'Choose Disk Format', 'Choose Disk Type', 'Specify Name and Location', 'Configure Disk' (highlighted), and 'Summary'. The main area has a title 'Configure Disk' with a disk icon. Below the title, it says 'You can create a blank virtual hard disk or copy the contents of an existing physical disk.' There are two radio buttons: 'Create a new blank virtual hard disk' (selected) and 'Copy the contents of the specified physical disk:'. The 'Create a new blank virtual hard disk' option has a 'Size:' field with '30' entered and '(Maximum: 64 TB)' in parentheses. The 'Copy the contents of the specified physical disk:' option has a table listing physical drives and their sizes. The table has two columns: 'Physical Hard Disk' and 'Size'. The rows are: '\\.\\PHYSICALDRIVE0' (1863 GB), '\\.\\PHYSICALDRIVE1' (125 MB), '\\.\\PHYSICALDRIVE2' (125 MB), '\\.\\PHYSICALDRIVE3' (125 MB), and '\\.\\PHYSICALDRIVE4' (125 MB). Below the table, there is a radio button for 'Copy the contents of the specified virtual hard disk' and a 'Path:' field with a 'Browse...' button. At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

**Configure Disk**

Before You Begin  
Choose Disk Format  
Choose Disk Type  
Specify Name and Location  
**Configure Disk**  
Summary

You can create a blank virtual hard disk or copy the contents of an existing physical disk.

☒ Create a new blank virtual hard disk  
Size:  GB (Maximum: 64 TB)

☐ Copy the contents of the specified physical disk:

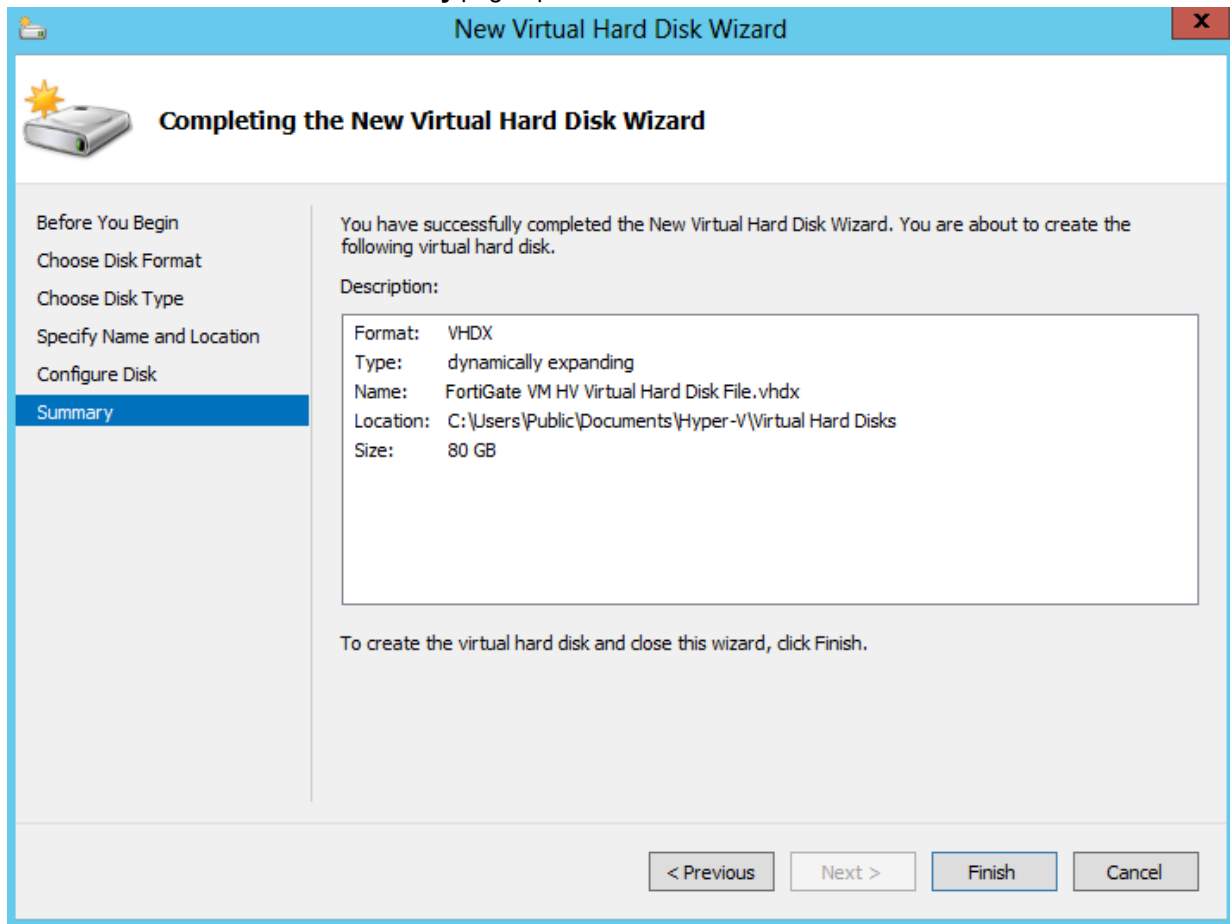
Physical Hard Disk	Size
\\.\PHYSICALDRIVE0	1863 GB
\\.\PHYSICALDRIVE1	125 MB
\\.\PHYSICALDRIVE2	125 MB
\\.\PHYSICALDRIVE3	125 MB
\\.\PHYSICALDRIVE4	125 MB

☐ Copy the contents of the specified virtual hard disk  
Path:

< Previous   Next >   Finish   Cancel

7. Select to **Create a new blank virtual hard disk** and enter the size of the disk in GB. The maximum size is dependent on your server environment.

Select **Next** to continue. The **Summary** page opens.



8. The summary page provides details of the virtual hard disk. Select **Finish** to create the virtual hard disk.
9. Select **Apply** to save the settings and select **OK** to exit the settings page.

## High availability Hyper-V configuration

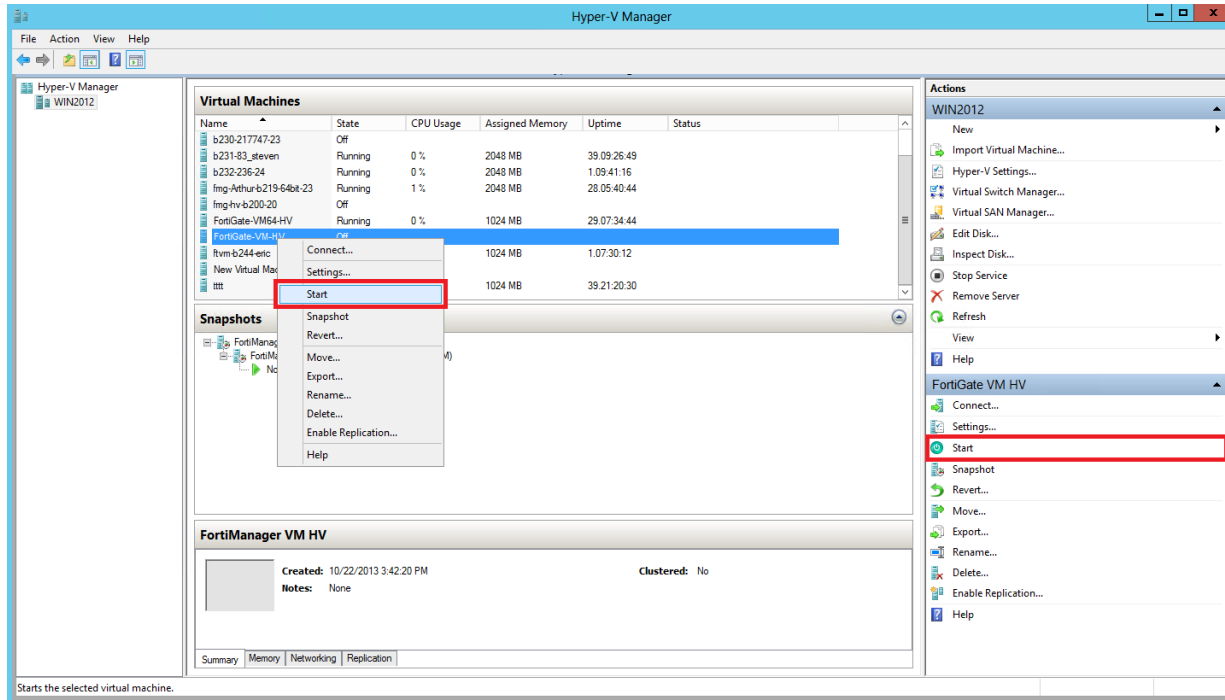
Promiscuous mode and support for MAC address spoofing is required for FortiGate-VM for Hyper-V to support FortiGate Clustering Protocol (FGCP) high availability (HA). By default the FortiGate-VM for Hyper-V has promiscuous mode enabled in the XML configuration file in the FortiGate-VM Hyper-V image. If you have problems with HA mode, confirm that this is still enabled.

In addition, because the FGCP applies virtual MAC addresses to FortiGate data interfaces and because these virtual MAC addresses mean that matching interfaces of different FortiGate-VM instances will have the same virtual MAC addresses you have to configure Hyper-V to allow MAC spoofing. But you should only enable MAC spoofing for FortiGate-VM data interfaces. You should not enable MAC spoofing for FortiGate HA heartbeat interfaces.

With promiscuous mode enabled and the correct MAC spoofing settings you should be able to configure HA between two or more FortiGate-VM for Hyper-V instances.

## Start the FortiGate VM

You can now proceed to power on your FortiGate VM. Select the name of the FortiGate VM in the list of virtual machines, right-click, and select **Start** in the menu. Optionally, you can select the name of the FortiGate VM in the list of virtual machines and select **Start** in the **Actions** menu.



# Deployment example – KVM

Once you have downloaded the FORTINET.out.kvm.zip file and extracted virtual hard drive image file fortios.qcow2, you can create the virtual machine in your KVM environment.

The following topics are included in this section:

- [Create the FortiGate VM virtual machine](#)
- [Configure FortiGate VM hardware settings](#)
- [Start the FortiGate VM](#)

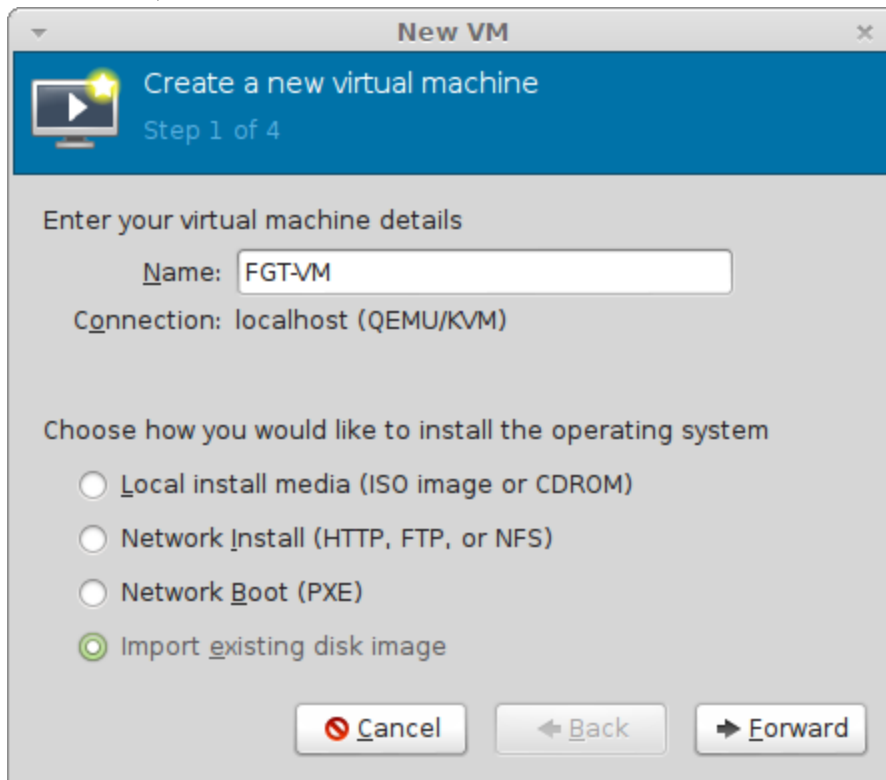
## Create the FortiGate VM virtual machine

**To create the FortiGate VM virtual machine:**

1. Launch Virtual Machine Manager (virt-manager) on your KVM host server.

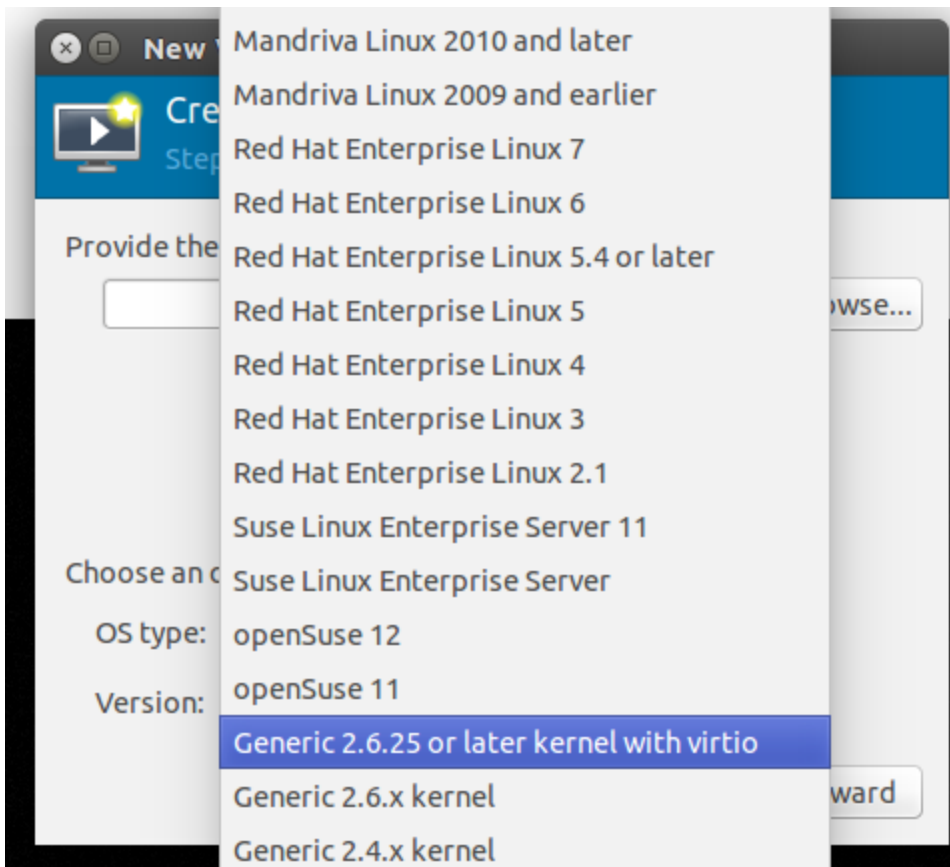
The **Virtual Machine Manager** home page opens.

2. In the toolbar, select **Create a new virtual machine**.



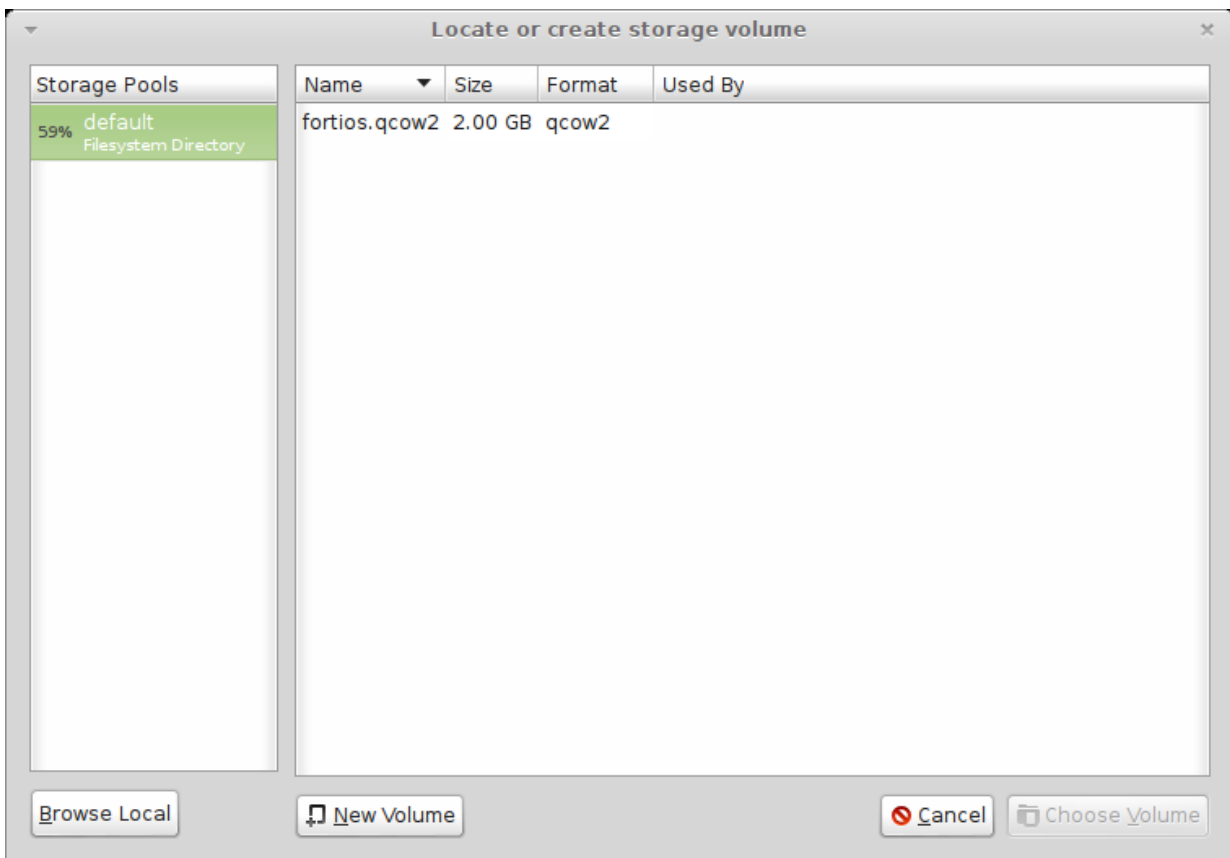
3. Enter a **Name** for the VM, FGT-VM for example.
4. Ensure that **Connection** is localhost. (This is the default.)
5. Select **Import existing disk image**.

6. Select **Forward**.



7. In **OS Type** select **Linux**.

8. In **Version**, select a Generic version with virtio.

9. Select **Browse**.

10. If you copied the fortios.qcow2 file to `/var/lib/libvirt/images`, it will be visible on the right. If you saved it somewhere else on your server, select **Browse Local** and find it.
11. Choose **Choose Volume**.
12. Select **Forward**.
13. Specify the amount of memory and number of CPUs to allocate to this virtual machine. The amounts must not exceed your license limits. See [Virtual FortiOS overview on page 8](#).
14. Select **Forward**.
15. Expand **Advanced options**. A new virtual machine includes one network adapter by default. Select a network adapter on the host computer. Optionally, set a specific MAC address for the virtual network interface. Set **Virt Type** to **virtio** and **Architecture** to **qcow2**.
16. Select **Finish**.

## Configure FortiGate VM hardware settings

Before powering on your FortiGate VM you must add the log disk and configure the virtual hardware of your FortiGate VM.

**To configure settings for FortiGate VM on the server:**

1. In the Virtual Machine Manager, locate the name of the virtual machine and then select **Open** from the toolbar.
2. Select **Add Hardware**. In the **Add Hardware** window select **Storage**.



3. Select **Create a disk image on the computer's hard drive** and set the size to 30GB.



If you know your environment will expand in the future, it is recommended to increase the hard disk size beyond 30GB. The VM license limit is 2TB.

---

4. Enter:

<b>Device type</b>	Virtio disk
<b>Cache mode</b>	Default
<b>Storage format</b>	raw



Even though raw is the storage format listed, the qcow2 format is also supported.

---

5. Select **Network** to configure add more the network interfaces. The **Device type** must be **Virtio**.

A new virtual machine includes one network adapter by default. You can add more through the Add Hardware window. FortiGate VM requires four network adapters. You can configure network adapters to connect to a virtual switch or to network adapters on the host computer.

6. Select **Finish**.

## Start the FortiGate VM

You can now proceed to power on your FortiGate VM. Select the name of the FortiGate VM in the list of virtual machines. In the toolbar, select **Console** and then select **Start**.

# Deployment example – Open Xen

Once you have downloaded the FORTINET.out.Open Xen.zip file and extracted virtual hard drive image file fortios.qcow2, you can create the virtual machine in your OpenXen environment.

The following topics are included in this section:

[Create the FortiGate VM virtual machine](#)

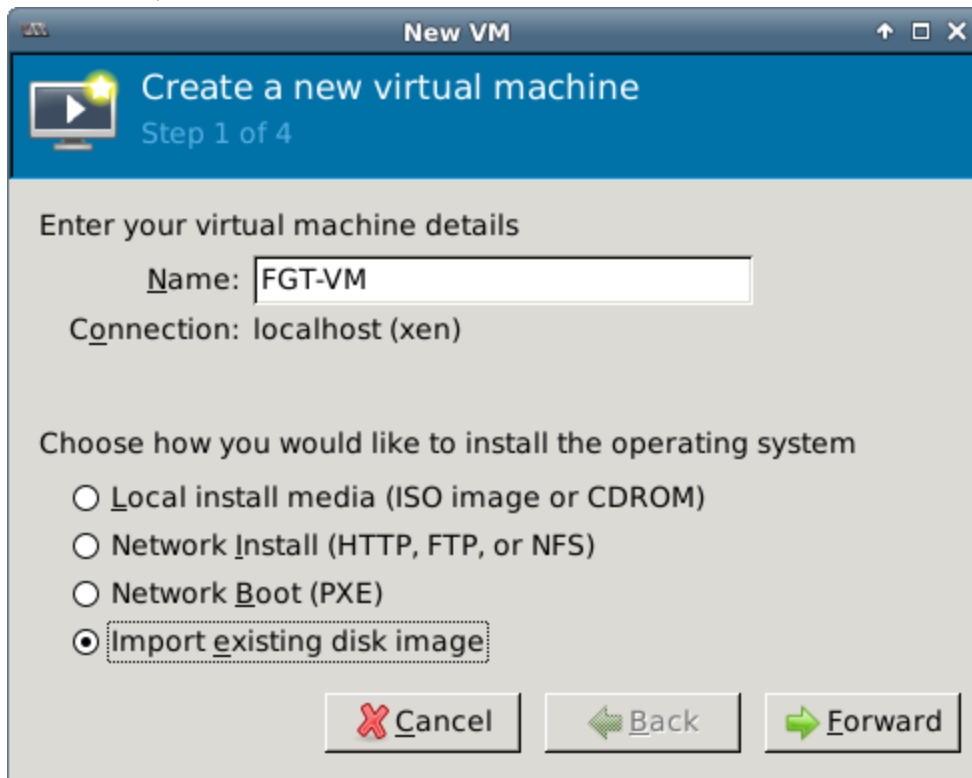
## Create the FortiGate VM virtual machine

**To create the FortiGate VM virtual machine:**

1. Launch Virtual Machine Manager (virt-manager) on your Open Xen host server.

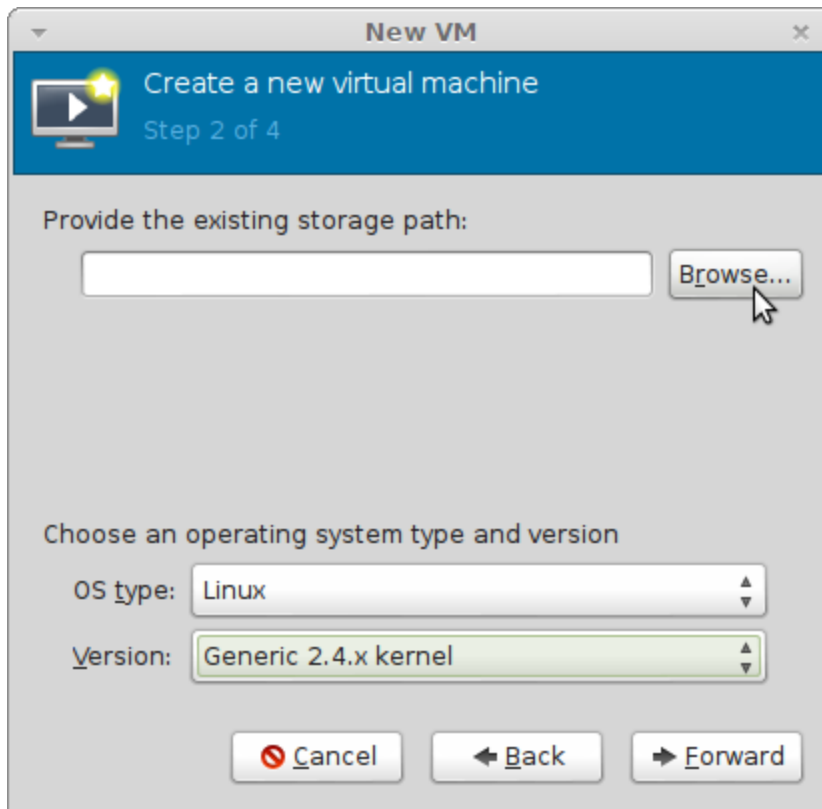
The **Virtual Machine Manager** home page opens.

2. In the toolbar, select **Create a new virtual machine**.



3. Enter a **Name** for the VM, FGT-VM for example.
4. Ensure that **Connection** is localhost. (This is the default.)
5. Select **Import existing disk image**.

6. Select **Forward**.



7. In **OS Type** select **Linux**.

8. In **Version**, select **Generic 2.4.x.kernel**.

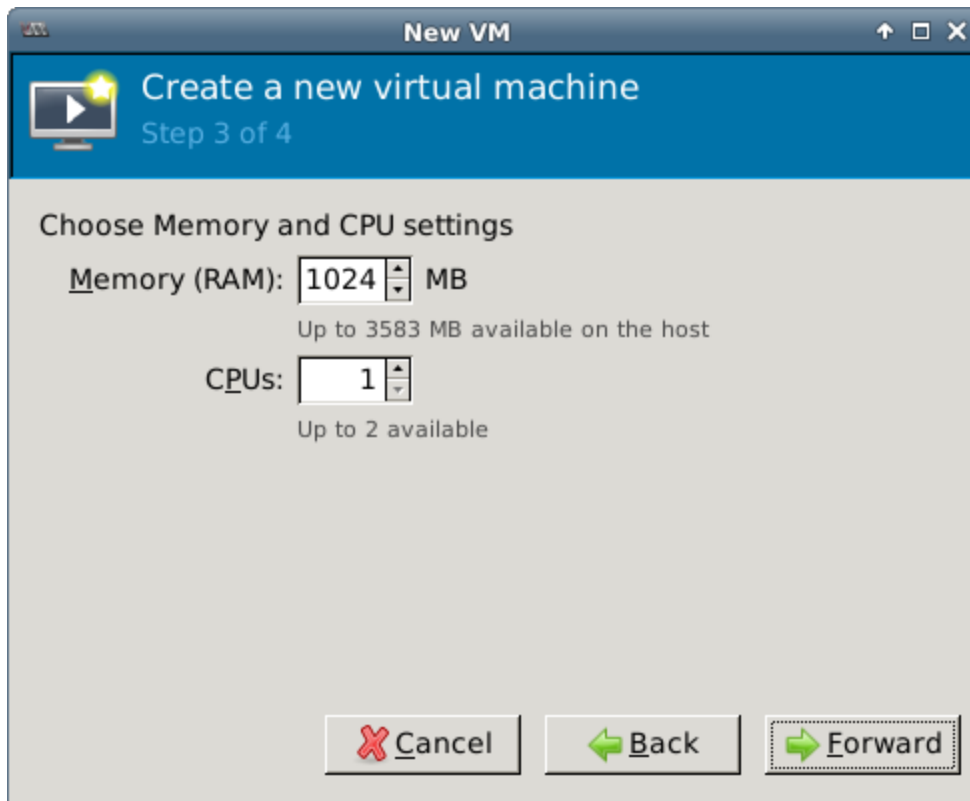
9. Select **Browse**.

The **Locate or create storage volume** window opens.

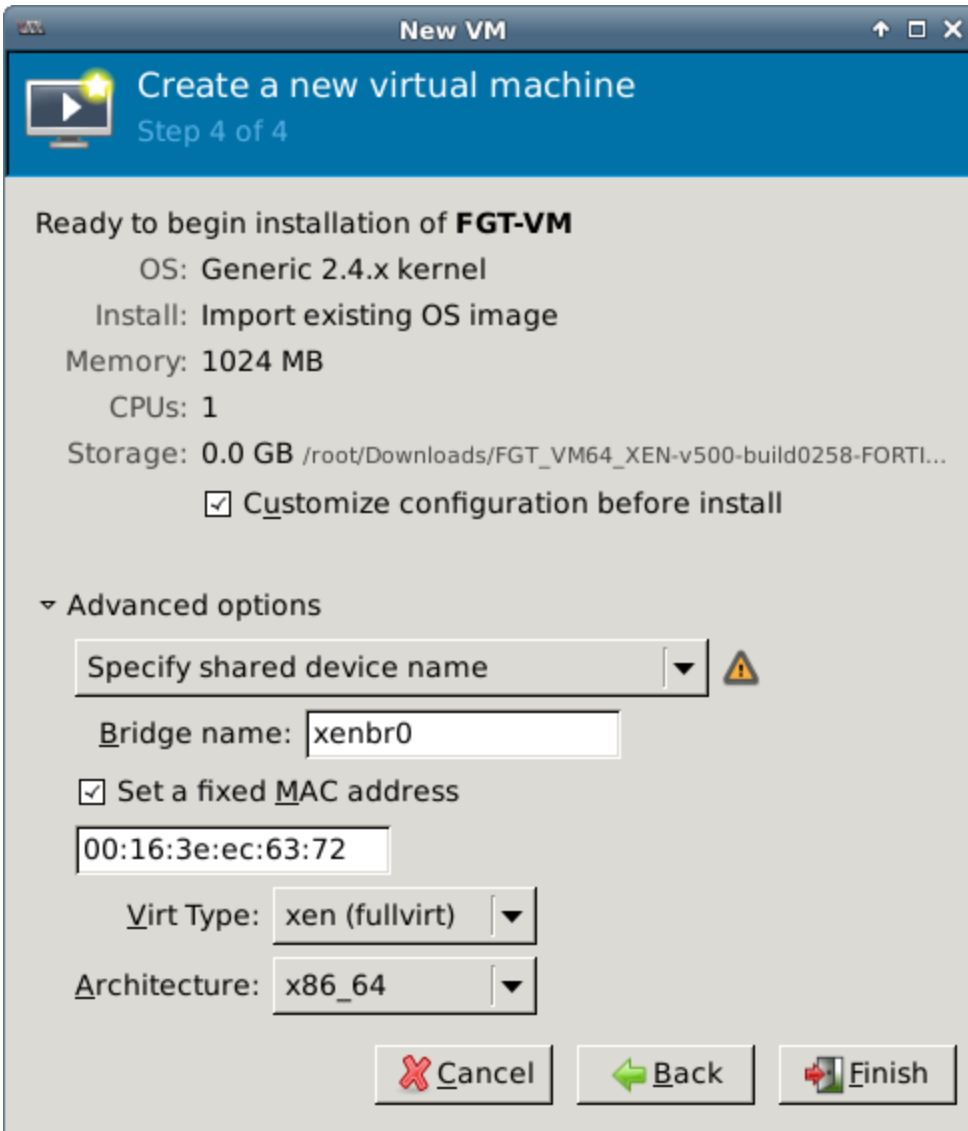
10. Select **Browse Local**, find the fortios.qcow2 disk image file.

11. Select fortios.qcow2 and select **Choose Volume**.

12. Select **Forward**.



13. Specify the amount of memory and number of CPUs to allocate to this virtual machine. The amounts must not exceed your license limits.

**14. Select Forward.**

New VM

Create a new virtual machine  
Step 4 of 4

Ready to begin installation of **FGT-VM**

OS: Generic 2.4.x kernel  
Install: Import existing OS image  
Memory: 1024 MB  
CPUs: 1  
Storage: 0.0 GB /root/Downloads/FGT\_VM64\_XEN-v500-build0258-FORTI...

☒ Customize configuration before install

▼ Advanced options

Specify shared device name ▼ ⚠

Bridge name: xenbr0

☒ Set a fixed MAC address

00:16:3e:ec:63:72

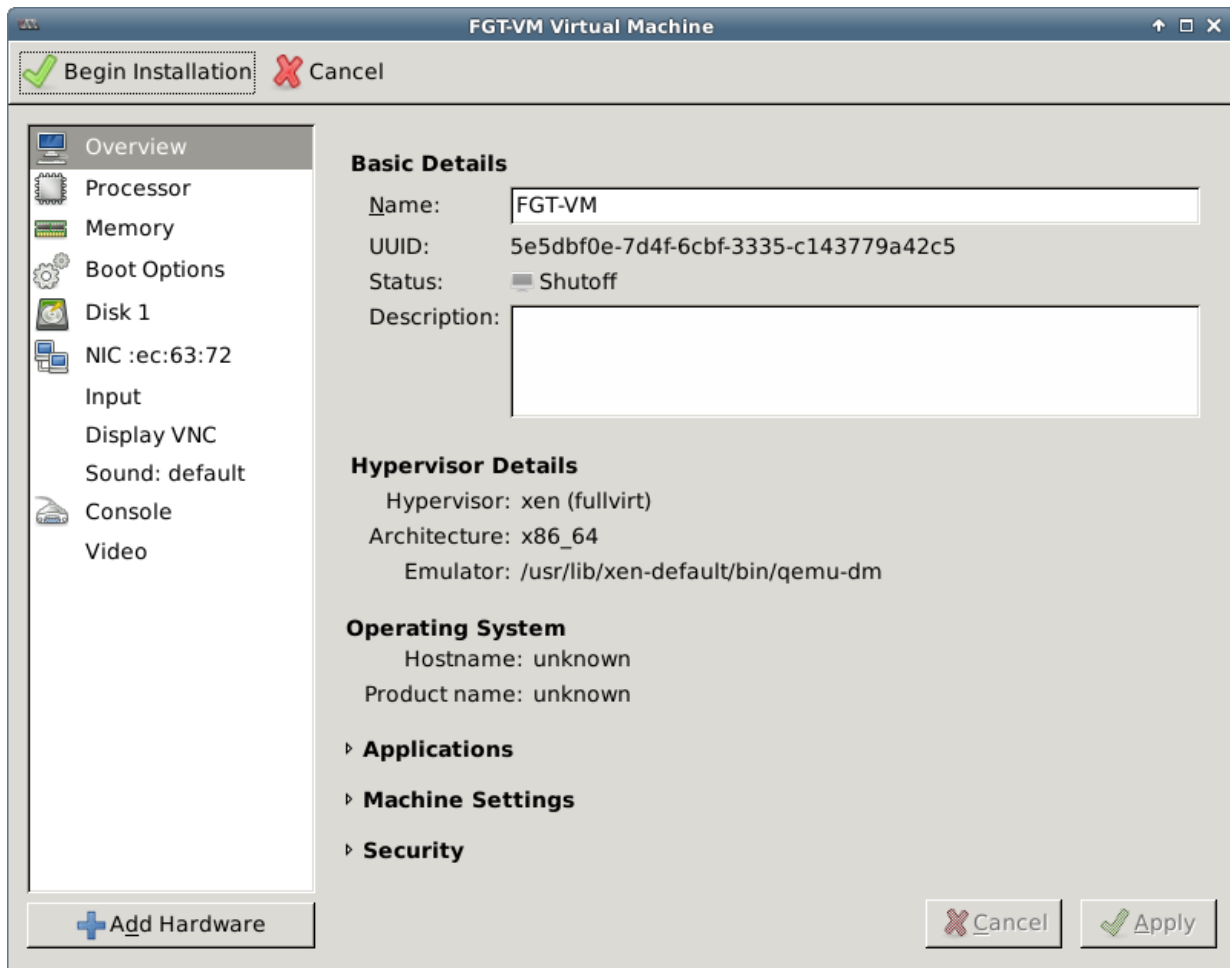
Virt Type: xen (fullvirt) ▼

Architecture: x86\_64 ▼

Cancel Back Finish

- 15. Select *Customize configuration before install*.** This enables you to make some hardware configuration changes before VM creation is started.
- 16. Expand *Advanced options*.** A new virtual machine includes one network adapter by default. Select **Specify shared device name** and enter the name of the bridge interface on the Open Xen host. Optionally, set a specific MAC address for the virtual network interface. **Virt Type** and **Architecture** are set by default and should be correct.
- 17. Select *Finish*.**

The virtual machine hardware configuration window opens.



You can use this window to add hardware such as network interfaces and disk drives.

18. Select **Add Hardware**. In the **Add Hardware** window select **Storage**.
19. Select **Create a disk image on the computer's hard drive** and set the size to 30GB.



If you know your environment will expand in the future, it is recommended to increase the hard disk size beyond 30GB. The VM license limit is 2TB.

20. Enter:

<b>Device type</b>	Virtio disk
<b>Cache mode</b>	Default
<b>Storage format</b>	raw

21. Select **Network** to configure add more the network interfaces. The **Device type** must be **Virtio**.

A new virtual machine includes one network adapter by default. You can add more through the Add Hardware window. FortiGate VM requires four network adapters. You can configure network adapters to connect to a virtual

switch or to network adapters on the host computer.

**22. Select **Finish**.**

**23. Select **Begin Installation**.** After the installation completes successfully, the VM starts and the console window opens.

# Deployment example – Citrix XenServer

Once you have downloaded the FORTINET.out.CitrixXen.zip file and extracted the files, you can create the virtual machine in your Citrix Xen environment.

The following topics are included in this section:

[Create the FortiGate VM virtual machine \(XenCenter\)](#)

[Configure virtual hardware](#)

## Create the FortiGate VM virtual machine (XenCenter)

### To create the FortiGate VM virtual machine from the OVF file

1. Launch XenCenter on your management computer.

The management computer can be any computer that can run Citrix XenCenter, a Windows application.

2. If you have not already done so, select **ADD a server**. Enter your Citrix XenServer IP address and the root logon credentials required to manage that server.

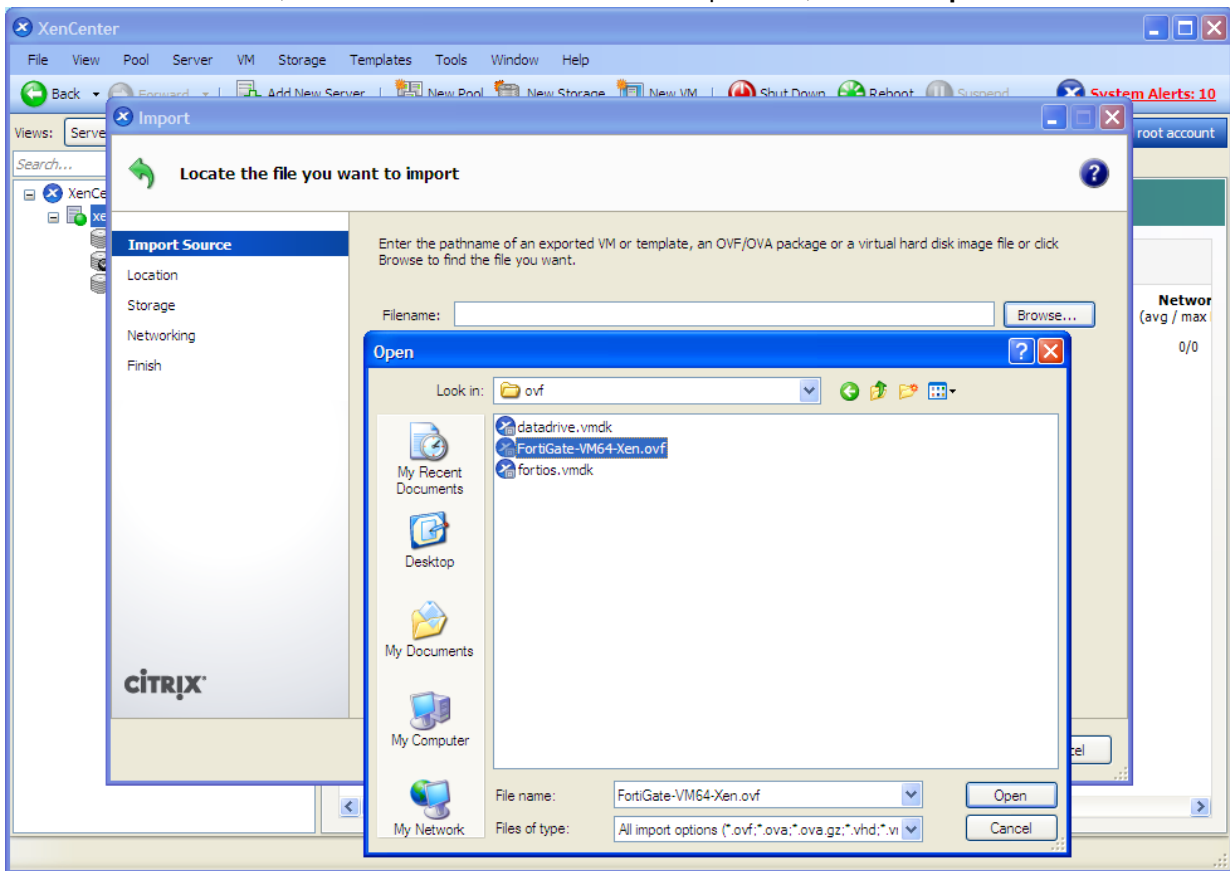
Your Citrix XenServer is added to the list in the left pane.

The **Virtual Machine Manager** home page opens.

3. Go to **File > Import**. An import dialog will appear.

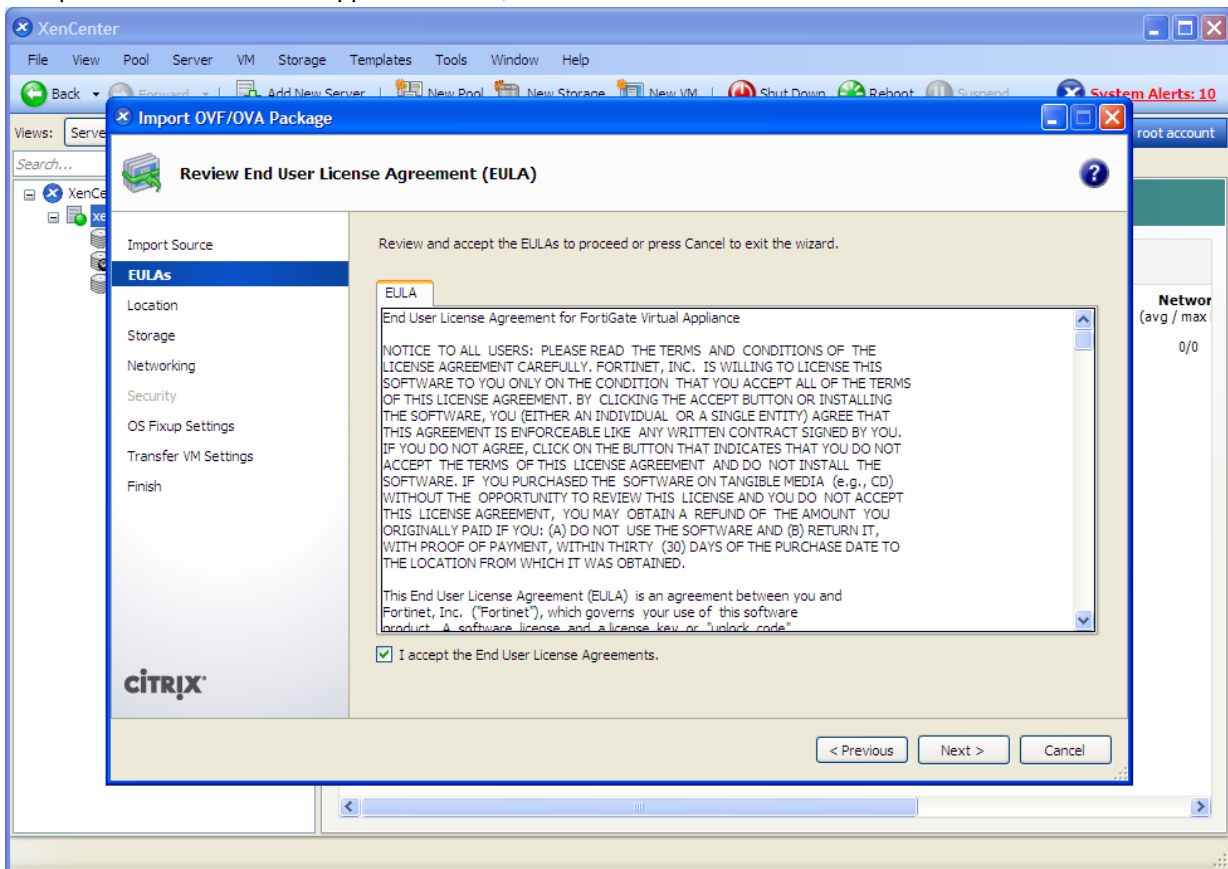


- Click the **Browse** button, find the FortiGate-VM64-Xen.ovf template file, then click **Open**.



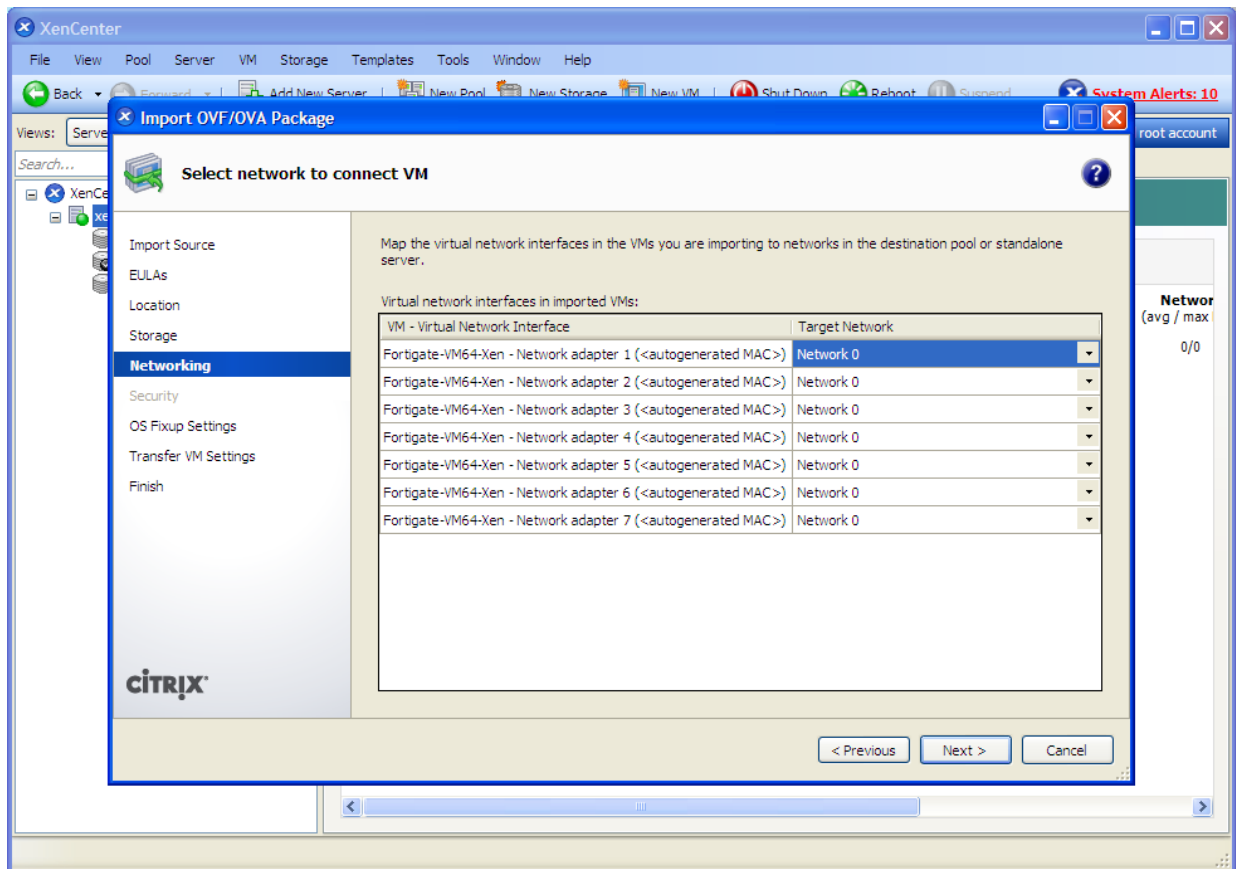
- Select **Next**.

6. Accept the FortiGate Virtual Appliance EULA, then select **Next**.



7. Choose the pool or standalone server that will host the VM, then select **Next**.
8. Select the storage location for FortiGate VM disk drives or accept the default. Select **Next**.

9. Configure how each vNIC (virtual network adapter) in FortiGate VM will be mapped to each vNetwork on the Citrix XenServer, then click **Next**.



10. Click **Next** to skip OS fixup.
11. Select **Next** to use the default network settings for transferring the VM to the host.
12. Select **Finish**.

The Citrix XenServer imports the FortiGate VM files and configures the VM as specified in the OVF template. Depending on your computer's hardware speed and resource load, and also on the file size and speed of the network connection, this might take several minutes to complete.



When VM import is complete, the XenCenter left pane includes the FortiGate VM in the list of deployed VMs for your Citrix XenServer.

## Configure virtual hardware

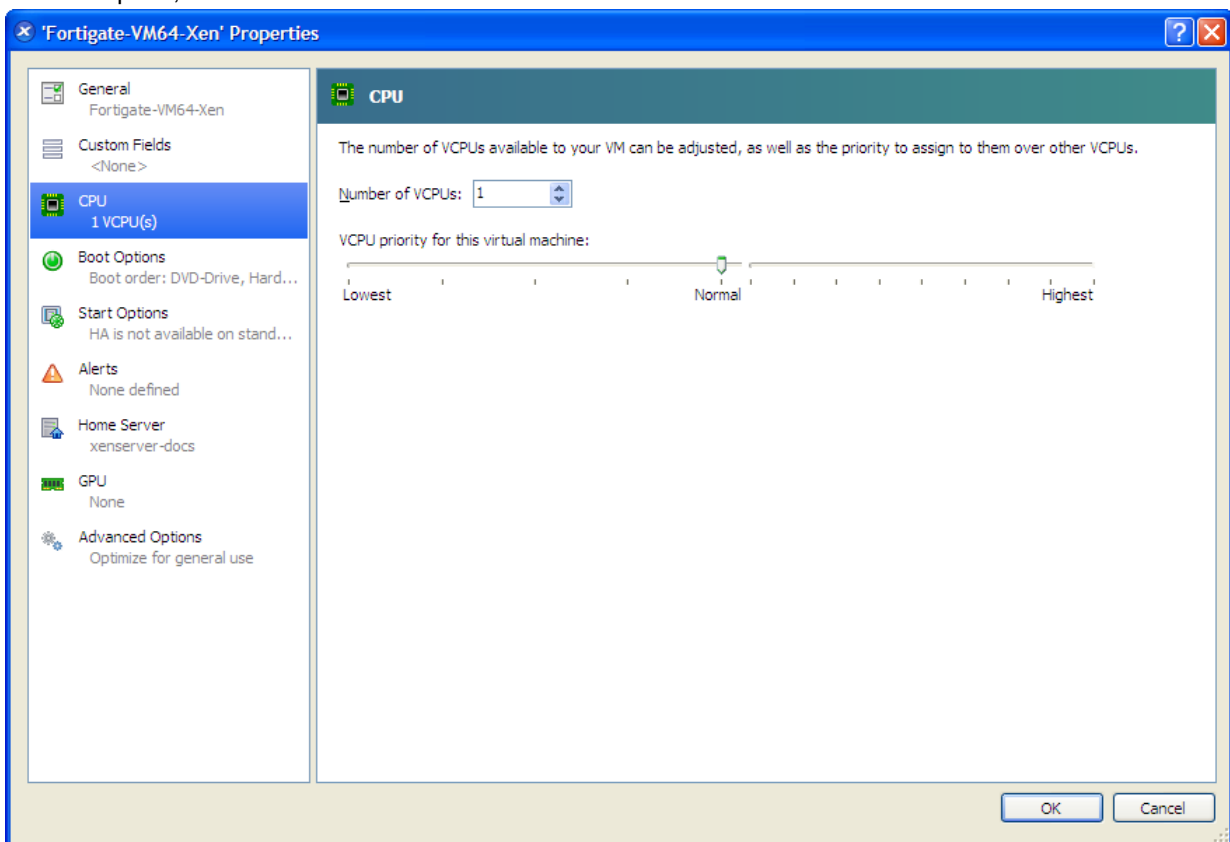
Before you start your FortiGate-VM for the first time, you need to adjust your virtual machine's virtual hardware settings to meet your network requirements.

### Configuring number of CPUs and memory size

Your FortiGate-VM license limits the number CPUs and amount of memory that you can use. The amounts you allocate must not exceed your license limits.

#### To access virtual machine settings

1. Open XenCenter.
2. Select your FortiGate VM in the left pane.  
The tabs in the right pane provide access to the virtual hardware configuration. The Console tab provides access to the FortiGate console.
1. To set the number of CPUs
2. In the XenCenter left pane, right-click the FortiGate VM and select Properties.  
The Properties window opens.
3. In the left pane, select CPU.

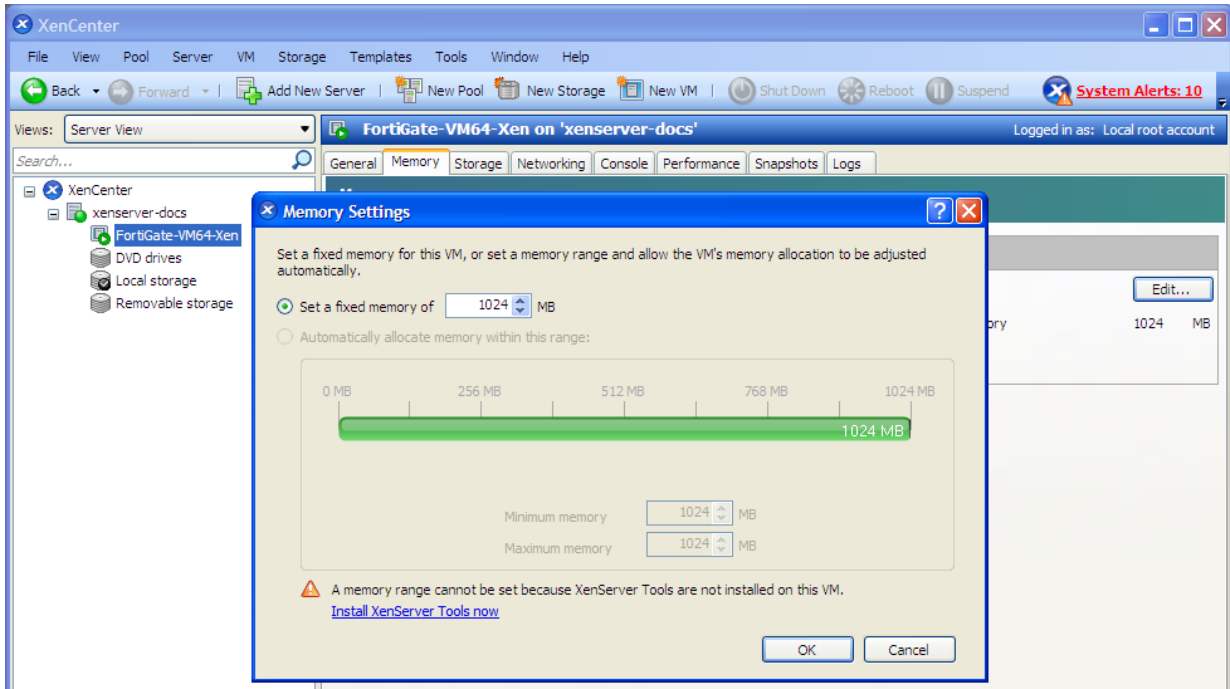


4. Adjust **Number of CPUs** and then select **OK**.

XenCenter will warn if you select more CPUs than the Xen host computer contains. Such a configuration might reduce performance.

### To set memory size

1. In the XenCenter left pane, select the FortiGate VM.
2. In the right pane, select the **Memory** tab.
3. Select **Edit**, modify the value in the **Set a fixed memory of** field and select **OK**.



## Configuring disk storage

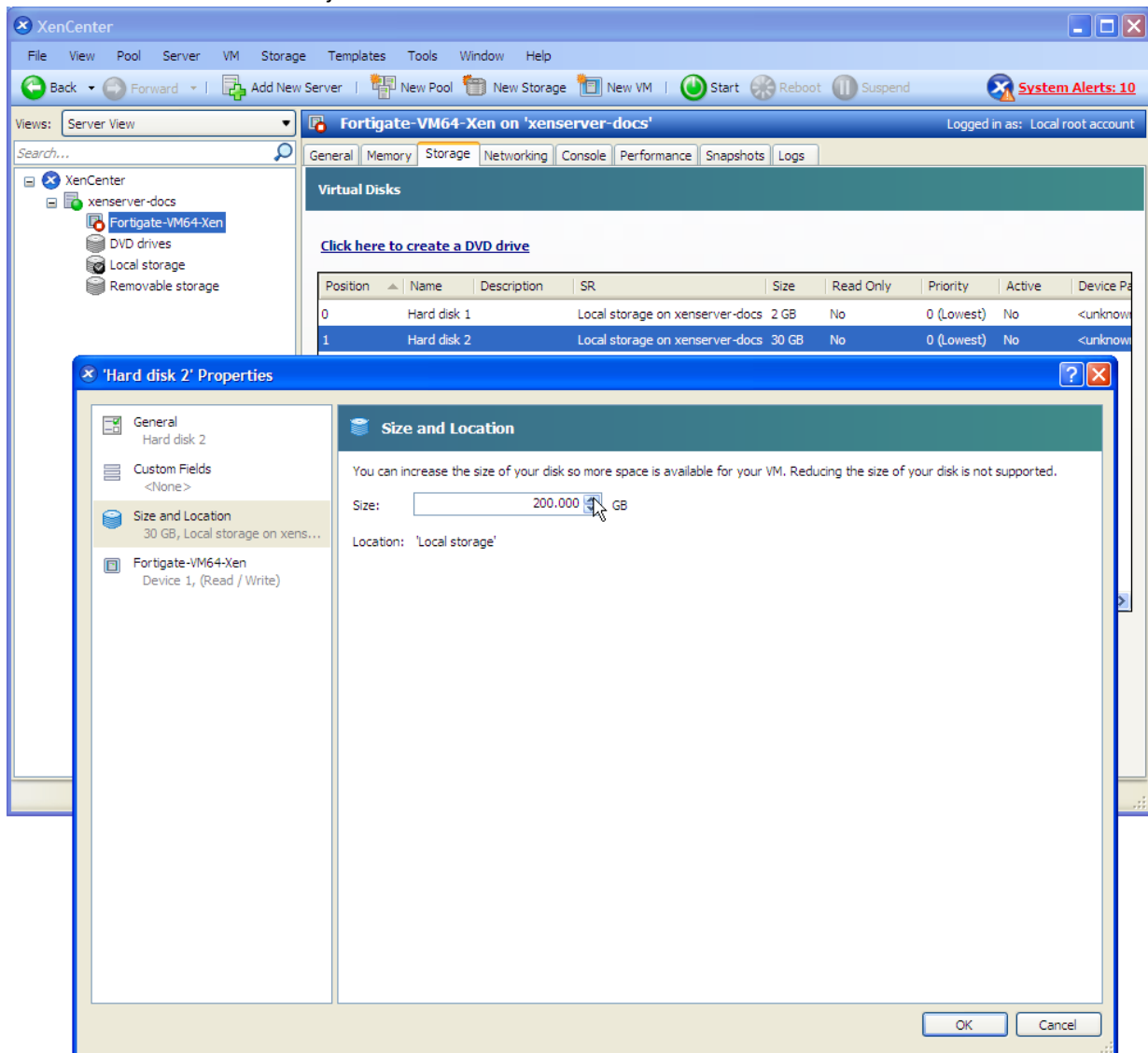
By default the FortiGate VM data disk 30GB. You will probably want to increase this. Disk resizing must be done before you start the VM for the first time.

### To resize the FortiGate data disk

1. In the XenCenter left pane, select the FortiGate VM.
2. Select the **Storage** tab. Select **Hard disk 2** (the 30GB drive), then select **Properties**.

The '**Hard disk 2**' **Properties** window opens.

3. Select **Size and Location**. Adjust **Size** and select **OK**.



# FortiGate VM initial configuration

Before you can connect to the FortiGate VM web-based manager you must configure a network interface in the FortiGate VM console. Once an interface with administrative access is configured, you can connect to the FortiGate VM web-based Manager and upload the FortiGate VM license file that you downloaded from the [Customer Service & Support](#) website.

The following topics are included in this section:

[Set FortiGate VM port1 IP address](#)

[Connect to the FortiGate VM web-based manager](#)

[Upload the FortiGate VM license file](#)

[Validate the FortiGate VM license with FortiManager](#)

[Configure your FortiGate VM](#)

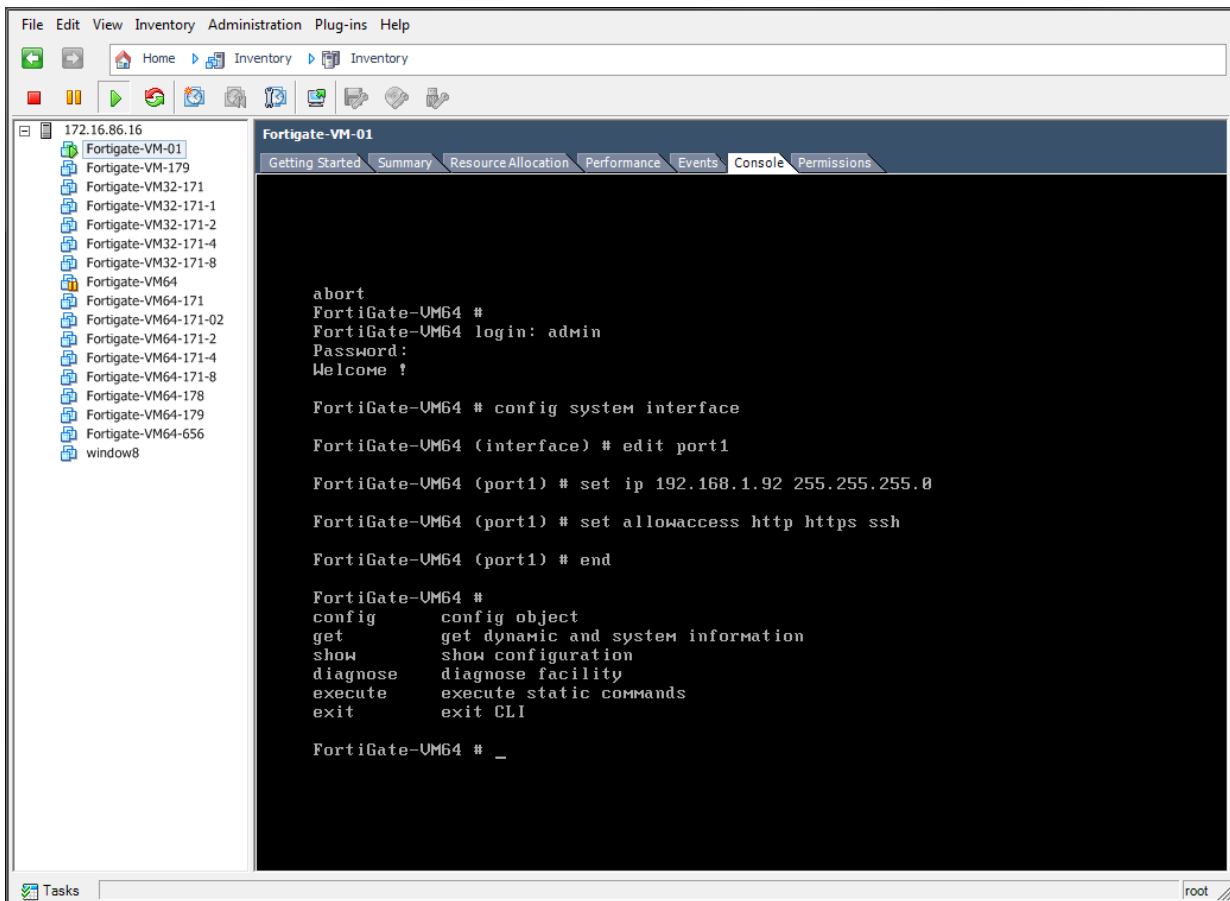
## Set FortiGate VM port1 IP address

Hypervisor management environments include a guest console window. On the FortiGate VM, this provides access to the FortiGate console, equivalent to the console port on a hardware FortiGate unit. Before you can access the Web-based manager, you must configure FortiGate VM port1 with an IP address and administrative access.

**To configure the port1 IP address:**

1. In your hypervisor manager, start the FortiGate VM and access the console window.  
You might need to press Return to see a login prompt.

**Example of FortiGate VM console access:**



2. At the FortiGate VM login prompt enter the username `admin`. By default there is no password. Just press Return.
3. Using CLI commands, configure the port1 IP address and netmask. Also, HTTP access must be enabled because until it is licensed the FortiGate VM supports only low-strength encryption. HTTPS access will not work.

For example:

```

config system interface
edit port1
set ip 192.168.0.100 255.255.255.0
append allowaccess http
end

```



You can also use the `append allowaccess` CLI command to enable other access protocols, such as `auto-ipsec`, `http`, `probe-response`, `radius-acct`, `snmp`, and `telnet`. The `ping`, `https`, `ssh`, and `fgfm` protocols are enabled on the `port1` interface by default.

4. To configure the default gateway, enter the following CLI commands:

```

config router static
edit 1
set device port1
set gateway <class_ip>
end

```





You must configure the default gateway with an IPv4 address. FortiGate VM needs to access the Internet to contact the FortiGuard Distribution Network (FDN) to validate its license.

5. To configure your DNS servers, enter the following CLI commands:

```
config system dns
  set primary <Primary DNS server>
  set secondary <Secondary DNS server>
end
```



The default DNS servers are 208.91.112.53 and 208.91.112.52.

6. To upload the FortiGate VM license from an FTP or TFTP server, use the following CLI command:

```
execute restore vmlicense {ftp | tftp} <VM license file name> <Server IP or FQDN>
[:server port]
```



You can also upload the license in the FortiGate VM Web-based Manager. See [Set FortiGate VM port1 IP address on page 71](#).

## Web-based Manager and Evaluation License dialog box

The screenshot displays the FortiGate VM Web-based Manager interface. On the left is a navigation menu with categories like System, Network, Admin, and Router. The main panel shows 'System Information' and 'System Resources'. An 'Evaluation License' dialog box is open in the center, displaying the Fortinet logo and the following text:

**FORTINET**  
REAL TIME NETWORK PROTECTION  
**FortiGate-VM**  
You are currently in evaluation mode  
14 days until expiration

Below the dialog box, the 'License' section is visible, showing a table with the following data:

VM License	
Registration Status	Valid [Update]
CPUs Detected	1 / 1
Evaluation License Expires	Sat May 4 07:39:00 2013
Support Contract	
Registration	Unreachable
FortiGuard Services	
AntiVirus	Unreachable [Configure]
IPS & Application Control	Unreachable [Configure]

Buttons for 'Remind Later' and 'Enter License' are located at the bottom right of the dialog box. The background interface also shows system resources like CPU and Memory usage, and an alert message console at the bottom.

## Connect to the FortiGate VM web-based manager

When you have configured the port1 IP address and netmask, launch a web browser and enter the IP address that you configured for port1. At the login page, enter the username `admin` and password field and select **Login**. The default password is no password. The Web-based Manager will appear with an **Evaluation License** dialog box.



Due to low encryption on the FortiGate side of the connection, some modern browsers will not allow the connection. If that is the case, the adjusting of the browser settings is unlikely to make a difference. There are two options:

- Use FTP or TFTP to apply the license
- Make sure that the interface on the port being accessed has been configured to allow HTTP/HTTPS access

## Upload the FortiGate VM license file

Every Fortinet VM includes a 15-day trial license. During this time the FortiGate VM operates in evaluation mode. Before using the FortiGate VM you must enter the license file that you downloaded from the [Customer Service & Support](#) website upon registration.

### GUI

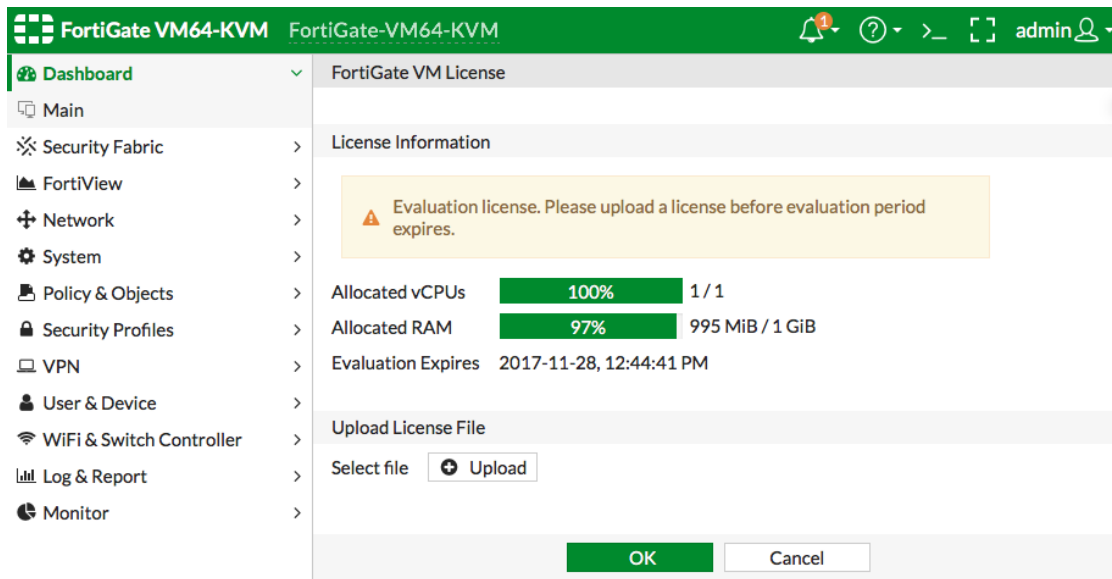
To upload the FortiGate VM license file:

1. There are 2 ways to get to the License upload window.
  - i. In the **Dashboard > Main** window, in the **Virtual Machine** widget, left click on the **FGVMEV** (FortiGate-VM Evaluation) **License** icon. This will reveal a menu of selections to take you to directly to the **FortiGate VM License** window or to the **FortiGuard Details** window.
  - ii. Go to **System > FortiGuard**. In the **Larcenist Information** section, go to the **Virtual Machine** row and click on the link to **FortiGate VM License**.

2. In the **Evaluation License** dialog box, select **Enter License**.

The license upload page opens.

**License upload page:**



3. Select **Upload** and locate the license file (.lic) on your computer. Select **OK** to upload the license file.
4. Refresh the browser to login.
5. Enter `admin` in the Name field and select **Login**. The VM registration status appears as valid in the License Information widget once the license has been validated by the FortiGuard Distribution Network (FDN) or FortiManager for closed networks.



Modern browsers can have an issue with allowing connecting to a FortiGate if the encryption on the device is too low. Adjusting browser settings does not normally mitigate the issue. If this happens, Admins must use a FTP/TFTP server to apply the license.

## CLI

You can also upload the license file via the CLI using the following CLI command:

```
execute restore vmlicense {ftp | tftp} <filename string> <ftp server>[:ftp port]
```

### Example:

The following is an example output when using a tftp server to install license.

```
exec restore vmlicense tftp license.lic 10.0.1.2
This operation will overwrite the current VM license!Do you want to continue? (y/n)y
Please wait...Connect to tftp server 10.0.1.2 ...
Get VM license from tftp server OK.
VM license install succeeded.
Rebooting firewall.
```



The command has the side effect of rebooting the firewall without giving you a chance to back out or delay the reboot, so be careful about the timing of using the command.

## Validate the FortiGate VM license with FortiManager

You can validate your FortiGate VM license with some models of FortiManager. To determine whether your FortiManager unit has the VM Activation feature, see Features section of the [FortiManager Product Data sheet](#).

### To validate your FortiGate VM with your FortiManager:

1. To configure your FortiManager as a closed network, enter the following CLI command on your FortiManager:

```
config fmupdate publicnetwork
  set status disable
end
```

2. To configure FortiGate VM to use FortiManager as its override server, enter the following CLI commands on your FortiGate VM:

```
config system central-management
  set mode normal
  set type fortimanager
  set fmg <IPv4 address of the FortiManager device>
  set fmg-source-ip <Source IPv4 address when connecting to the FortiManager device>
  set include-default-servers disable
  set vdom <Enter the name of the VDOM to use when communicating with the FortiManager device>
end
```

3. Load the FortiGate VM license file in the Web-based Manager. Go to **System > Dashboard > Status**. In the **License Information** widget, in the **Registration Status** field, select **Update**. Browse for the `.lic` license file and select **OK**.

4. To activate the FortiGate VM license, enter the following CLI command on your FortiGate VM:

```
execute update-now
```

5. To check the FortiGate VM license status, enter the following CLI commands on your FortiGate VM:

```
get system status
```

The following output is displayed:

```
Version: Fortigate-VM v5.0,build0099,120910 (Interim)
Virus-DB: 15.00361(2011-08-24 17:17)
Extended DB: 15.00000(2011-08-24 17:09)
Extreme DB: 14.00000(2011-08-24 17:10)
IPS-DB: 3.00224(2011-10-28 16:39)
FortiClient application signature package: 1.456(2012-01-17 18:27)
Serial-Number: FGVM02Q105060000
License Status: Valid
BIOS version: 04000002
Log hard disk: Available
Hostname: Fortigate-VM
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Distribution: International
```

```
Branch point: 511
Release Version Information: MR3 Patch 4
System time: Wed Jan 18 11:24:34 2012

diagnose hardware sysinfo vm full
    The following output is displayed:
UUID: 564db33a29519f6b1025bf8539a41e92
valid: 1
status: 1
code: 200 (If the license is a duplicate, code 401 will be displayed)
warn: 0
copy: 0
received: 45438
warning: 0
recv: 201201201918
dup:
```

## Licensing timeout

In closed environments without Internet access, it is mandatory to perform offline licensing of the virtual FortiGate using a FortiManager as a license server. If the FortiGate-VM cannot perform license validation within the license timeout period, which is 30 days, the FortiGate will discard all packets and effectively ceasing operation as a firewall.

The status of the license will go through some status changes before it times out.

Status	Description
Valid	The FortiGate can connect and validate against a FortiManager or FDS
Warning	The FortiGate <b>cannot</b> connect and validate against a FortiManager or FDS. A check is made against how many days the Warning status has been continuous. If the number is less the 30 days the status does not change.
Invalid	The FortiGate <b>cannot</b> connect and validate against a FortiManager or FDS. A check is made against how many days the Warning status has been continuous. If the number is 30 days or more, the status changes to Invalid. The firewall ceases to function properly.



There is only a single log entry after the virtual FortiGate cannot access the license server for the license expiration period. This means that when you go searching the logs for a reason for the FortiGate being offline there will not be a long list of error logs that draw attention to the issue. There will only be the one entry.

## Configure your FortiGate VM

Once the FortiGate VM license has been validated you can begin to configure your device. You can use the **Wizard** located in the top toolbar for basic configuration including enabling central management, setting the admin password, setting the time zone, and port configuration.

For more information on configuring your FortiGate VM see the FortiOS Handbook at <http://docs.fortinet.com>.



**FORTINET®**



Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.